# *NWD310N*

*Wireless N PCI Adapter*

# *User's Guide*

Version 1.0
11/2007
Edition 1

ZyXEL

www.zyxel.com

# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the NWD310N using the ZyXEL utility. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Online Help
  Embedded web help for descriptions of individual screens and supplementary information.
- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

## User's Guide Feedback

Help us help you. Send all User's Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

# Document Conventions

### Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your NWD310N.

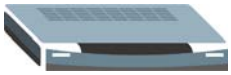
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

### Syntax Conventions

- The NWD310N may be referred to as the "NWD310N", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

### Icons Used in Figures

Figures in this User's Guide may use the following generic icons.

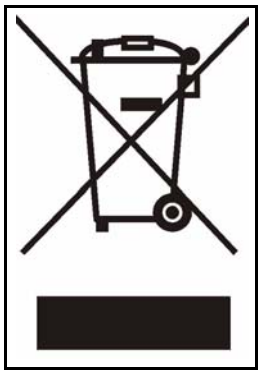
| | | |
|---|---|---|
| Wireless Access Point | Computer | Notebook computer |
| Server | Modem  | Telephone |
| Internet | Wireless Signal | |

# Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Ground yourself (by properly using an anti-static wrist strap, for example) whenever working with the device's hardware or connections.
- ONLY qualified service personnel should service or disassemble this device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.



# Contents Overview

**Introduction and Configuration ..... 19**

Getting Started ..... 21
Tutorial ..... 27
Wireless LANs ..... 37
Wireless Configuration ..... 47
Maintenance ..... 67

**Troubleshooting and Specifications ..... 71**

Troubleshooting ..... 73
Product Specifications ..... 77

**Appendices and Index ..... 79**

# Table of Contents

**About This User's Guide** ..... **3**

**Document Conventions** ..... **4**

**Safety Warnings** ..... **6**

**Contents Overview** ..... **7**

**Table of Contents** ..... **9**

**List of Figures** ..... **13**

**List of Tables** ..... **17**

**Part I: Introduction and Configuration** ..... **19**

**Chapter 1**
**Getting Started** ..... **21**

1.1 About Your NWD310N ..... 21
1.1.1 Hardware ..... 21
1.2 Application Overview ..... 23
1.2.1 Infrastructure ..... 23
1.2.2 Ad-Hoc ..... 23
1.3 Hardware and Utility Installation ..... 24
1.3.1 ZyXEL Utility Icon ..... 24
1.4 Configuration Methods ..... 25
1.4.1 Enabling Windows Wireless Configuration ..... 25
1.4.2 Accessing the ZyXEL Utility ..... 26

**Chapter 2**
**Tutorial** ..... **27**

2.1 Connecting to an AP using Wi-Fi Protected Setup (WPS) ..... 27
2.1.1 Push Button Configuration (PBC) ..... 27
2.1.2 PIN Configuration ..... 29
2.2 Connecting to an AP Without Using WPS ..... 32
2.2.1 Manually Connecting to a Wireless LAN ..... 32
2.2.2 Creating and Using a Profile ..... 34

**Chapter 3**
**Wireless LANs** ..... **37**

3.1 Wireless LAN Overview ..... 37
3.2 Wireless LAN Security ..... 38
3.2.1 User Authentication and Encryption ..... 38
3.3 WiFi Protected Setup ..... 40
3.3.1 Push Button Configuration ..... 40
3.3.2 PIN Configuration ..... 41
3.3.3 How WPS Works ..... 42
3.3.4 Limitations of WPS ..... 45

**Chapter 4**
**Wireless Configuration ..... 47**

4.1 ZyXEL Utility Screen Summary ..... 47
4.2 The Link Info Screen ..... 47
4.2.1 Trend Chart ..... 49
4.3 The Site Survey Screen ..... 49
4.3.1 Security Settings ..... 51
4.3.2 Server Certificate Setting Screen ..... 55
4.3.3 Summary Screen ..... 55
4.4 The Profile Screen ..... 56
4.4.1 Adding a New Profile ..... 58
4.5 The Adapter Screen ..... 61
4.5.1 WPS: PBC (Push Button Configuration) ..... 62
4.5.2 WPS: PIN - Use this Device's PIN ..... 63
4.5.3 WPS: PIN - Use the PIN from the AP or Wireless Router ..... 63
4.6 Security Settings in Windows Vista ..... 64
4.6.1 Using PEAP in Vista ..... 64
4.6.2 Using TLS in Vista ..... 65

**Chapter 5**
**Maintenance ..... 67**

5.1 The About Screen ..... 67
5.2 Uninstalling the ZyXEL Utility ..... 67
5.3 Upgrading the ZyXEL Utility ..... 68

**Part II: Troubleshooting and Specifications ..... 71**

**Chapter 6**
**Troubleshooting ..... 73**

6.1 Power, Hardware Connections, and LEDs ..... 73
6.2 Accessing the Utility ..... 73
6.3 Link Quality ..... 74

6.4 Problems Communicating with Other Computers ..... 74

**Chapter 7**
**Product Specifications ..... 77**

**Part III: Appendices and Index ..... 79**

Appendix A Setting up Your Computer's IP Address ..... 81

Appendix B Wireless LANs ..... 103

Appendix C Windows Wireless Management ..... 117

Appendix D Legal Information ..... 139

Appendix E Customer Support ..... 143

**Index ..... 149**

# List of Figures

Figure 1 The NWD310N ..... 22
Figure 2 Application: Infrastructure ..... 23
Figure 3 Application: Ad-Hoc ..... 24
Figure 4 ZyXEL Utility: System Tray Icon ..... 24
Figure 5 Enable WZC ..... 25
Figure 6 Infrastructure Network ..... 27
Figure 7 Example WPS Process: PBC Method ..... 29
Figure 8 Example WPS Process: PIN Method ..... 31
Figure 9 ZyXEL Utility: Site Survey ..... 32
Figure 10 ZyXEL Utility: Security Settings ..... 33
Figure 11 ZyXEL Utility: Summary ..... 33
Figure 12 ZyXEL Utility: Link Info ..... 33
Figure 13 ZyXEL Utility: Profile ..... 34
Figure 14 ZyXEL Utility: Add New Profile ..... 34
Figure 15 ZyXEL Utility: Profile Security ..... 35
Figure 16 ZyXEL Utility: Profile Encryption ..... 35
Figure 17 ZyXEL Utility: Profile Summary ..... 35
Figure 18 ZyXEL Utility: Profile Activate ..... 36
Figure 19 Example of a Wireless Network ..... 37
Figure 20 Example WPS Process: PIN Method ..... 42
Figure 21 How WPS works ..... 43
Figure 22 WPS: Example Network Step 1 ..... 44
Figure 23 WPS: Example Network Step 2 ..... 44
Figure 24 WPS: Example Network Step 3 ..... 45
Figure 25 ZyXEL Utility Menu Summary ..... 47
Figure 26 Link Info ..... 48
Figure 27 Link Info: Trend Chart ..... 49
Figure 28 Site Survey ..... 50
Figure 29 Security Setting: WEP ..... 51
Figure 30 Security Setting: WPA-PSK/WPA2-PSK ..... 52
Figure 31 Security Settings: WPA/WPA2 ..... 53
Figure 32 Security Setting: 802.1x ..... 54
Figure 33 Server Certificate Setting Screen ..... 55
Figure 34 Summary Screen ..... 56
Figure 35 Profile ..... 57
Figure 36 Profile: Add a New Profile ..... 58
Figure 37 Profile: Wireless Settings ..... 59
Figure 38 Profile: Wireless Settings ..... 60

Figure 39 Profile: Security Settings ..... 60
Figure 40 Profile: Confirm New Settings ..... 60
Figure 41 Profile: Activate the Profile ..... 61
Figure 42 Adapter ..... 61
Figure 43 WPS: PBC (Push Button Configuration) ..... 62
Figure 44 WPS: PIN - Use this Device's PIN ..... 63
Figure 45 WPS: PIN - Use the PIN from the AP or Wireless Router ..... 64
Figure 46 Vista Security: Additional Information Required ..... 65
Figure 47 Vista Security: Enter Credentials ..... 65
Figure 48 Vista Security: Additional Information Required ..... 66
Figure 49 Vista Security: Select Certificate ..... 66
Figure 50 About ..... 67
Figure 51 Uninstall: Confirm ..... 68
Figure 52 Uninstall: Finish ..... 68
Figure 53 WIndows 95/98/Me: Network: Configuration ..... 82
Figure 54 Windows 95/98/Me: TCP/IP Properties: IP Address ..... 83
Figure 55 Windows 95/98/Me: TCP/IP Properties: DNS Configuration ..... 84
Figure 56 Windows XP: Start Menu ..... 85
Figure 57 Windows XP: Control Panel ..... 85
Figure 58 Windows XP: Control Panel: Network Connections: Properties ..... 86
Figure 59 Windows XP: Local Area Connection Properties ..... 86
Figure 60 Windows XP: Internet Protocol (TCP/IP) Properties ..... 87
Figure 61 Windows XP: Advanced TCP/IP Properties ..... 88
Figure 62 Windows XP: Internet Protocol (TCP/IP) Properties ..... 89
Figure 63 Windows Vista: Start Menu ..... 90
Figure 64 Windows Vista: Control Panel ..... 90
Figure 65 Windows Vista: Network And Internet ..... 90
Figure 66 Windows Vista: Network and Sharing Center ..... 90
Figure 67 Windows Vista: Network and Sharing Center ..... 91
Figure 68 Windows Vista: Local Area Connection Properties ..... 91
Figure 69 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties ..... 92
Figure 70 Windows Vista: Advanced TCP/IP Properties ..... 93
Figure 71 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties ..... 94
Figure 72 Macintosh OS 8/9: Apple Menu ..... 95
Figure 73 Macintosh OS 8/9: TCP/IP ..... 95
Figure 74 Macintosh OS X: Apple Menu ..... 96
Figure 75 Macintosh OS X: Network ..... 97
Figure 76 Red Hat 9.0: KDE: Network Configuration: Devices ..... 98
Figure 77 Red Hat 9.0: KDE: Ethernet Device: General ..... 98
Figure 78 Red Hat 9.0: KDE: Network Configuration: DNS ..... 99
Figure 79 Red Hat 9.0: KDE: Network Configuration: Activate ..... 99
Figure 80 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 ..... 100
Figure 81 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 ..... 100

Figure 82 Red Hat 9.0: DNS Settings in resolv.conf ..... 100
Figure 83 Red Hat 9.0: Restart Ethernet Card ..... 100
Figure 84 Red Hat 9.0: Checking TCP/IP Properties ..... 101
Figure 85 Peer-to-Peer Communication in an Ad-hoc Network ..... 103
Figure 86 Basic Service Set ..... 104
Figure 87 Infrastructure WLAN ..... 105
Figure 88 RTS/CTS ..... 106
Figure 89 WPA(2) with RADIUS Application Example ..... 113
Figure 90 WPA(2)-PSK Authentication ..... 114
Figure 91 Vista: Start Menu ..... 117
Figure 92 Vista: The Connect To Window ..... 118
Figure 93 Vista: Additional Information ..... 118
Figure 94 Vista: Enter Security Key ..... 119
Figure 95 Vista: Connecting ..... 119
Figure 96 Vista: Successful Connection ..... 120
Figure 97 Vista: Choose a Connection Option ..... 121
Figure 98 Vista: Connect Manually ..... 121
Figure 99 Vista: Successfully Added Network ..... 122
Figure 100 Vista: Set Up An Ad-hoc Network ..... 123
Figure 101 Vista: Ad-hoc Options ..... 123
Figure 102 Vista: Ad-hoc Network Ready ..... 124
Figure 103 Windows XP SP1: Wireless Network Connection Status ..... 125
Figure 104 Windows XP SP2: Wireless Network Connection Status ..... 125
Figure 105 Windows XP SP1: Wireless Network Connection Properties ..... 126
Figure 106 Windows XP SP2: Wireless Network Connection Properties ..... 126
Figure 107 Windows XP SP2: WZC Not Available ..... 127
Figure 108 Windows XP SP2: System Tray Icon ..... 127
Figure 109 Windows XP SP2: Wireless Network Connection Status ..... 128
Figure 110 Windows XP SP1: Wireless Network Connection Status ..... 128
Figure 111 Windows XP SP2: Wireless Network Connection ..... 129
Figure 112 Windows XP SP1: Wireless Network Connection Properties ..... 130
Figure 113 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK ..... 130
Figure 114 Windows XP SP2: Wireless Network Connection: No Security ..... 131
Figure 115 Windows XP: Wireless (network) properties: Association ..... 131
Figure 116 Windows XP: Wireless (network) properties: Authentication ..... 133
Figure 117 Windows XP: Protected EAP Properties ..... 134
Figure 118 Windows XP: Smart Card or other Certificate Properties ..... 135
Figure 119 Windows XP SP2: Wireless Networks: Preferred Networks ..... 136
Figure 120 Windows XP SP1: Wireless Networks: Preferred Networks ..... 136

# List of Tables

Table 1 NWD310N External View ..... 22
Table 2 NWD310N LEDs ..... 22
Table 3 ZyXEL Utility: System Tray Icon ..... 25
Table 4 ZyXEL Utility Menu Summary ..... 47
Table 5 Link Info ..... 48
Table 6 Link Info: Trend Chart ..... 49
Table 7 Site Survey ..... 50
Table 8 Security Setting: WEP ..... 51
Table 9 Security Setting: WPA-PSK/WPA2-PSK ..... 52
Table 10 Security Setting: WPA/WPA2 ..... 53
Table 11 Security Settings: IEEE 802.1x ..... 54
Table 12 Server Certificate Setting ..... 55
Table 13 Summary Screen ..... 56
Table 14 Profile ..... 57
Table 15 Profile: Add a New Profile ..... 58
Table 16 Profile: Wireless Settings ..... 59
Table 17 Adapter ..... 61
Table 18 WPS: PIN - Use this Device's PIN ..... 63
Table 19 WPS: PIN - Use the PIN from the AP or Wireless Router ..... 64
Table 20 About ..... 67
Table 21 Product Specifications ..... 77
Table 22 IEEE 802.11g ..... 107
Table 23 Wireless Security Levels ..... 108
Table 24 Comparison of EAP Authentication Types ..... 111
Table 25 Wireless Security Relational Matrix ..... 114
Table 26 Vista: Connect Manually ..... 121
Table 27 Windows XP SP2: System Tray Icon ..... 127
Table 28 Windows XP SP2: Wireless Network Connection ..... 129
Table 29 Windows XP: Wireless Networks ..... 131
Table 30 Windows XP: Wireless (network) properties: Association ..... 132
Table 31 Windows XP: Wireless (network) properties: Authentication ..... 133
Table 32 Windows XP: Protected EAP Properties ..... 134
Table 33 Windows XP: Smart Card or other Certificate Properties ..... 135

# PART I
# Introduction and Configuration

Getting Started (21)
Tutorial (27)
Wireless LANs (37)
Wireless Configuration (47)
Maintenance (67)

# 1

# Getting Started

This chapter introduces the NWD310N and prepares you to use the ZyXEL utility. The ZyXEL utility is a tool that helps you configure your NWD310N.

## 1.1 About Your NWD310N

Your NWD310N is an IEEE 802.11n draft 2.0 compliant wireless LAN adapter. It can also connect to IEEE 802.11b/g wireless networks. The NWD310N is WPS (Wi-Fi Protected Setup) compliant. WPS allows you to easily connect to another WPS-enabled device.

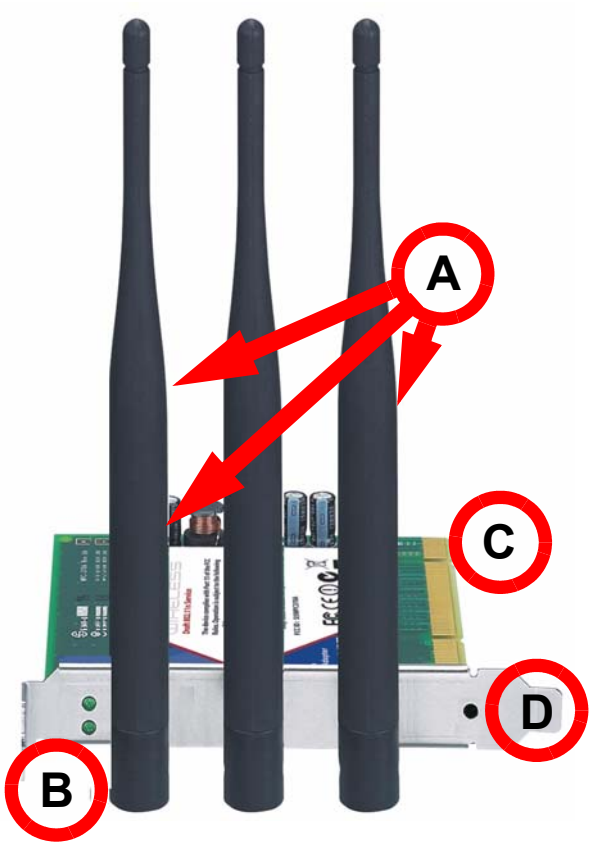
The NWD310N is a PCI adapter which occupies a PCI slot inside your desktop computer. The NWD310N also uses MIMO (Multiple-In, Multiple-Out) antenna technology to deliver high-speed wireless networking.

See your NWD310N's Quick Start Guide for installation instructions, and see the chapter on product specifications for detailed information.

### 1.1.1 Hardware

This section describes the NWD310N's physical appearance.

**Figure 1** The NWD310N




The following table describes the NWD310N.

**Table 1** NWD310N External View

| LABEL | DESCRIPTION |
|---|---|
| A | Removable antennas |
| B | LEDs (lights) |
| C | WPS button |
| D | PCI connector |

The following table describes the operation of the NWD310N's LEDs.

**Table 2** NWD310N LEDs

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| Link | Green | On | The NWD310N is connected to a wireless network. |
| | | Off | The NWD310N is not connected to a wireless network. |
| Tx/Rx | Yellow | On | The NWD310N is connected to a wireless network. |
| | | Blinking | The NWD310N is connected to a wireless network and is sending or receiving data. |
| | | Off | The NWD310N is not connected to a wireless network. |

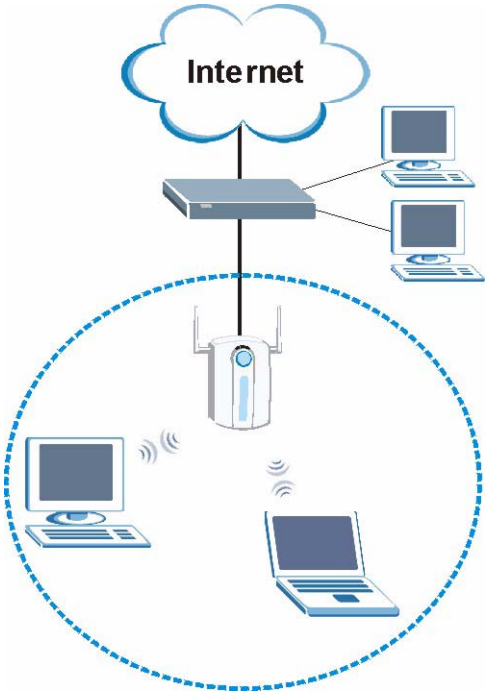
## 1.2 Application Overview

This section describes some network applications for the NWD310N. You can either set the network type to **Infrastructure** and connect to an AP or use **Ad-Hoc** mode and connect to a peer computer (another wireless device in Ad-Hoc mode).

### 1.2.1 Infrastructure

To connect to a network via an access point (AP), set the NWD310N network type to **Infrastructure** (see Chapter 4 on page 56). Through the AP, you can access the Internet or the wired network behind the AP.

**Figure 2** Application: Infrastructure



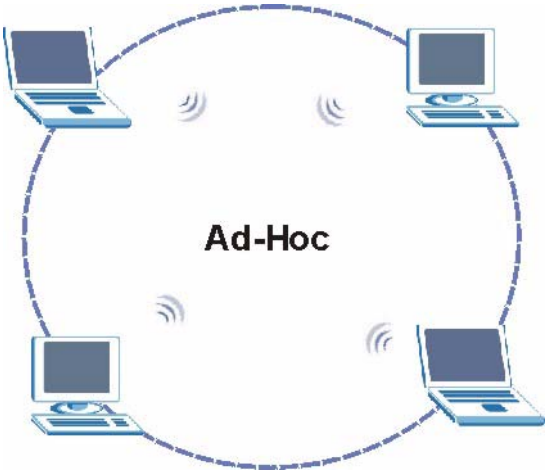

### 1.2.2 Ad-Hoc

To set up a small independent wireless workgroup without an AP, use **Ad-Hoc** (see Chapter 4 on page 56).

**Ad-Hoc** does not require an AP or a wired network. Two or more wireless clients communicate directly with each other.

Wi-Fi Protected Setup (WPS) is not available in ad-hoc mode.

**Figure 3** Application: Ad-Hoc




## 1.3 Hardware and Utility Installation

Follow the instructions in the Quick Start Guide to install the ZyXEL utility and make hardware connections.

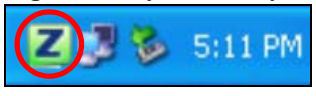
### 1.3.1 ZyXEL Utility Icon

After you install and start the ZyXEL utility, an icon for the ZyXEL utility appears in the system tray.

The ZyXEL utility system tray icon displays only when the NWD310N is installed properly.

When you use the ZyXEL utility, it automatically disables Wireless Zero Configuration (WZC) in Windows XP.

**Figure 4** ZyXEL Utility: System Tray Icon



The color of the ZyXEL utility system tray icon indicates the status of the NWD310N. Refer to the following table for details.

**Table 3** ZyXEL Utility: System Tray Icon

| COLOR | DESCRIPTION |
|---|---|
| Red | The NWD310N is not connected to a wireless network. |
| Green | The NWD310N is connected to a wireless network. |

## 1.4 Configuration Methods

To configure your NWD310N, use one of the following applications:

- Wireless Zero Configuration (WZC, the Windows XP wireless configuration tool) or WLAN AutoConfig (the Windows Vista wireless configuration tool).
- The ZyXEL utility.

Do NOT use Windows XP's Wireless Zero Configuration tool at the same time you use the ZyXEL utility.

### 1.4.1 Enabling Windows Wireless Configuration

When you use the ZyXEL utility, it automatically disables Windows XP's wireless configuration tool.

If you want to use the Windows XP wireless configuration tool to configure the NWD310N, you need to disable the ZyXEL utility. Right-click the utility icon ( ) in the system tray and select **Exit**.

**Figure 5** Enable WZC

Refer to the appendices for information on how to use the Windows wireless configuration tool to manage the NWD310N.

To reactivate the ZyXEL utility, double-click the ( ) icon on your desktop or click **Start**, **(All) Programs**, **ZyXEL Wireless N PCI Adapter Utility**, **ZyXEL Wireless N PCI Adapter Utility**.

## 1.4.2 Accessing the ZyXEL Utility

Double-click on the ZyXEL wireless LAN utility icon in the system tray to open the ZyXEL utility.

The ZyXEL utility screens are similar in all Microsoft Windows versions. Screens for Windows XP are shown in this User's Guide.

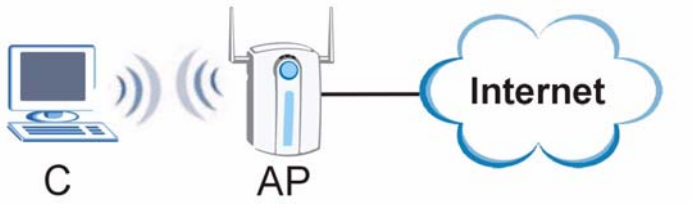
Click the icon (located in the top right corner) to display the online help window.

# 2

# Tutorial

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.

**Figure 6** Infrastructure Network




## 2.1 Connecting to an AP using Wi-Fi Protected Setup (WPS)

This section gives you an example of how to set up your wireless network using WPS. This example uses the NWD310N as the wireless client, and ZyXEL's NBG334W as the Access Point (AP).

The Access Point must be a WPS-aware device.

There are two WPS methods for creating a secure connection. This tutorial shows you both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 2.1.1 on page 27.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NWD310N's interface. See Section 2.1.2 on page 29. This is the more secure method, since one device can authenticate the other.

### 2.1.1 Push Button Configuration (PBC)

1. Make sure that your access point is turned on and that it is within range of the computer with the NWD310N installed.
2. Make sure that you have installed the NWD310N's driver and utility on your computer.

3 In the NWD310N's utility, click the **Adapter** tab, enable **WPS** and select **PBC (Push Button Configuration)**. In the screen that appears, click **Start**.

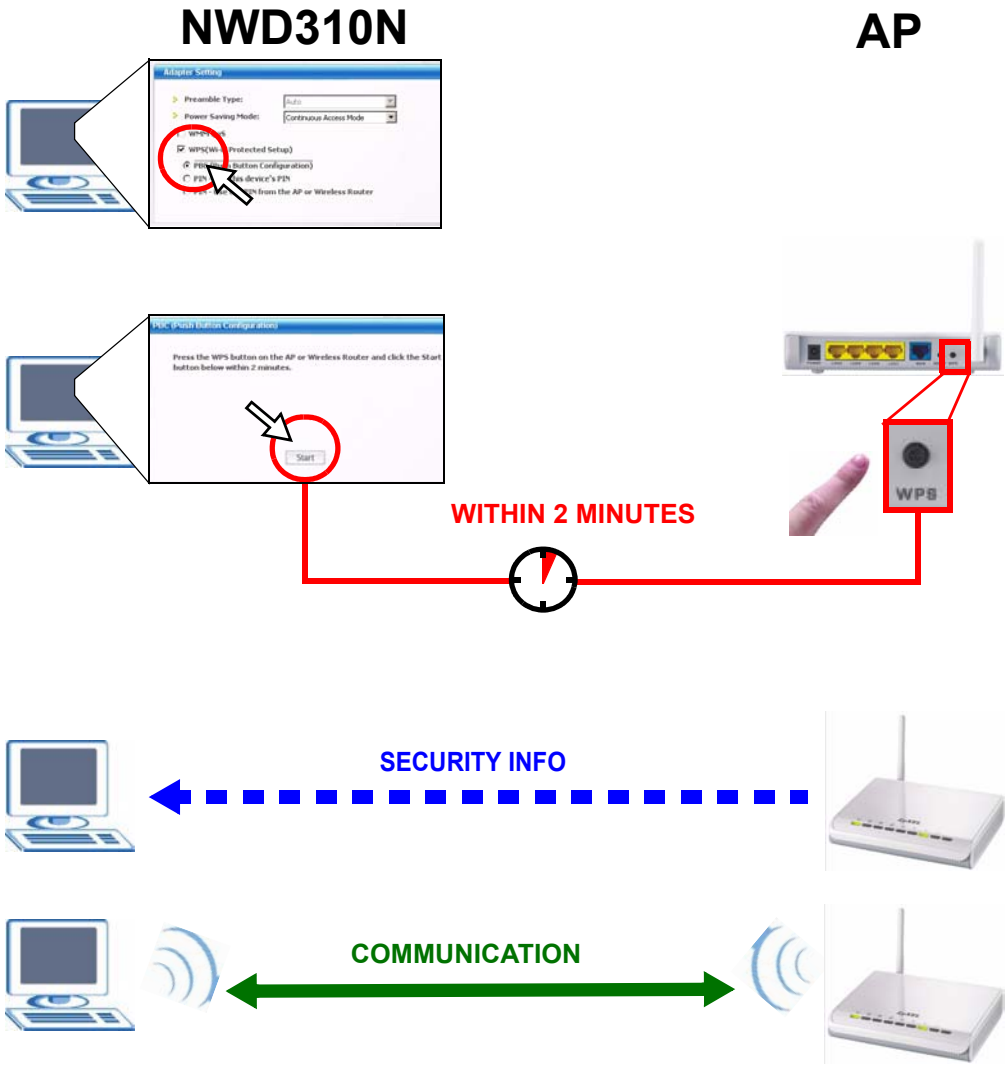
4 Log into the AP's web configurator and locate its WPS settings section. On the NBG334W, press the **Push Button** button in the **Network** > **Wireless Client** > **WPS Station** screen.

It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The AP sends the proper configuration settings to the NWD310N. This may take up to two minutes. Then the NWD310N is able to communicate with the AP securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both the AP (the NBG334W in this example) and the NWD310N.

**Figure 7** Example WPS Process: PBC Method




## 2.1.2 PIN Configuration

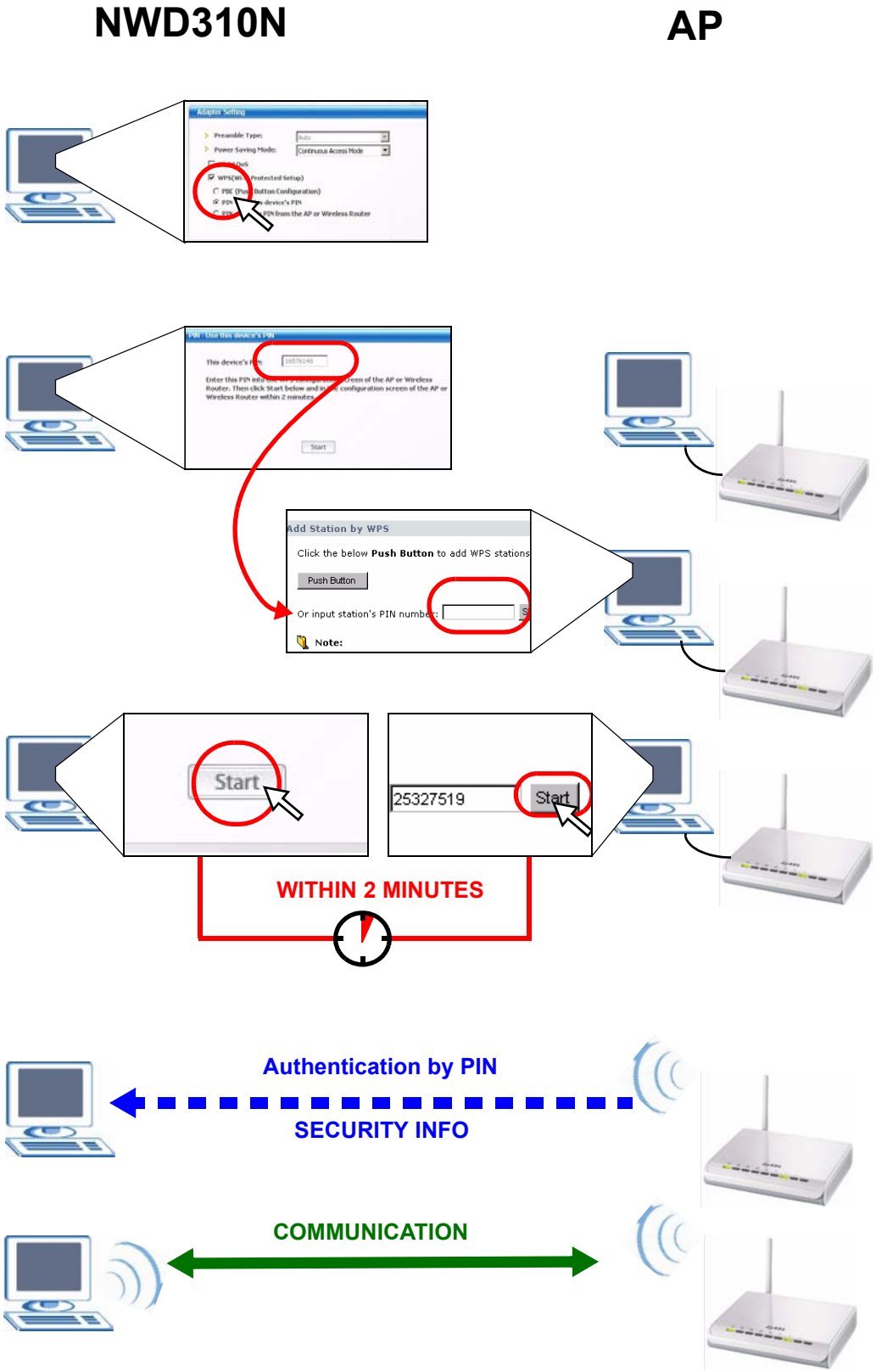
When you use the PIN configuration method, you need to use both the NWD310N's utility and the AP's configuration interface.

1. In the NWD310N's Adaptor tab, select **WPS** and **PIN - Use this Device's PIN**. Note down the PIN in the screen that appears.
2. Enter the PIN number in the AP's configuration interface. In the NBG334W, use the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen.
3. Click the **Start** buttons on both the NWD310N utility screen and the AP's configuration utility (the **WPS Station** screen on the NBG334W) within two minutes.

The NWD310N authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NWD310N securely.

The following figure shows you the example of configuring the wireless network and security on the NWD310N and the AP (ZyXEL's NBG334W in this example) by using the PIN method.

**Figure 8** Example WPS Process: PIN Method



## 2.2 Connecting to an AP Without Using WPS

There are three ways to connect the wireless client (the NWD310N) to a network without using WPS.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network (see Section 2.2.1 on page 32).
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer (see Section 2.2.2 on page 34).

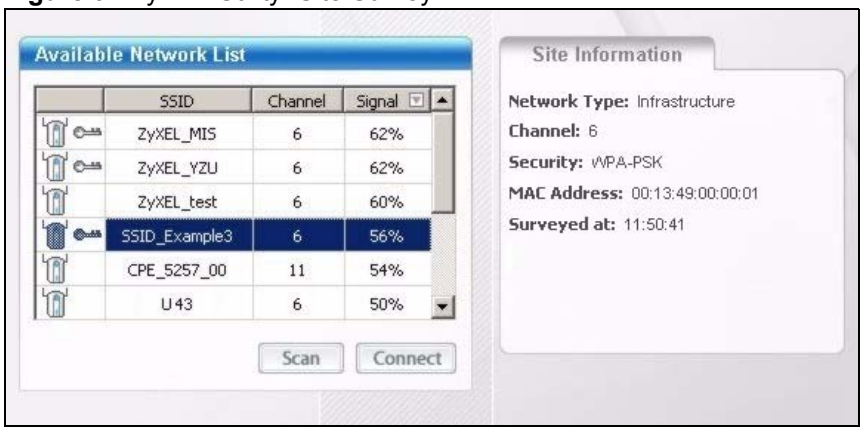
### 2.2.1 Manually Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

**Figure 9** ZyXEL Utility: Site Survey



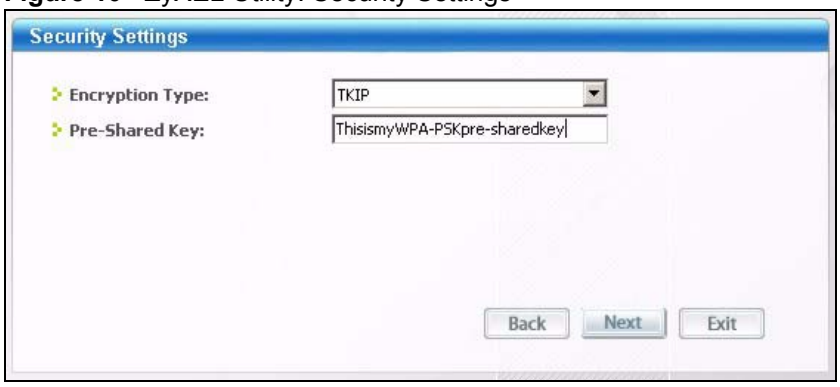

2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer. See Table 4.3 on page 49 for detailed field descriptions.

3 To connect to an AP or peer computer, either click an entry in the list and then click **Connect** or double-click an entry (**SSID_Example3** in this example).

4 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

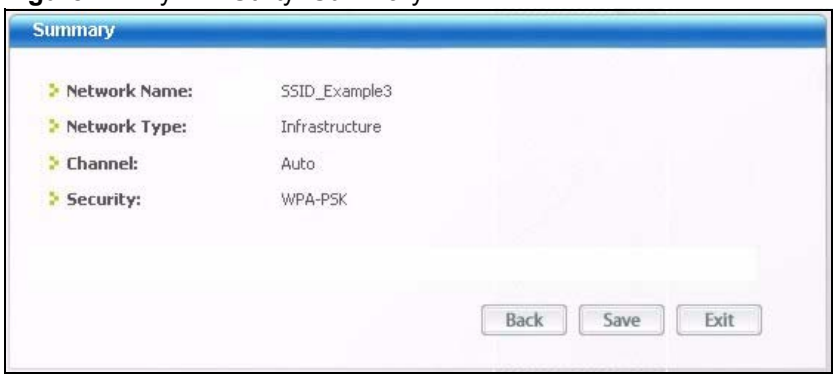
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

**Figure 10** ZyXEL Utility: Security Settings



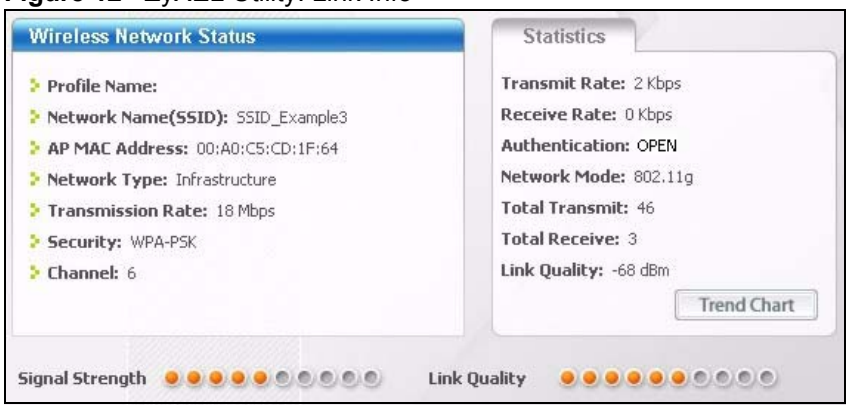

**5** The **Summary** window appears. Check your settings and click **Save** to continue.

**Figure 11** ZyXEL Utility: Summary




**6** The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank. See Table 4.2 on page 47 for detailed field descriptions.

**Figure 12** ZyXEL Utility: Link Info




**7** Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured. If you cannot access the web site, check the

Troubleshooting section of this User's Guide or contact your network administrator if necessary.

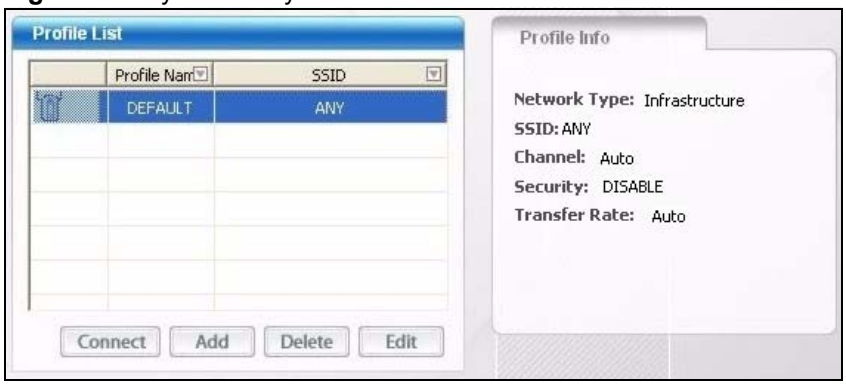
## 2.2.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the ZyXEL utility. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

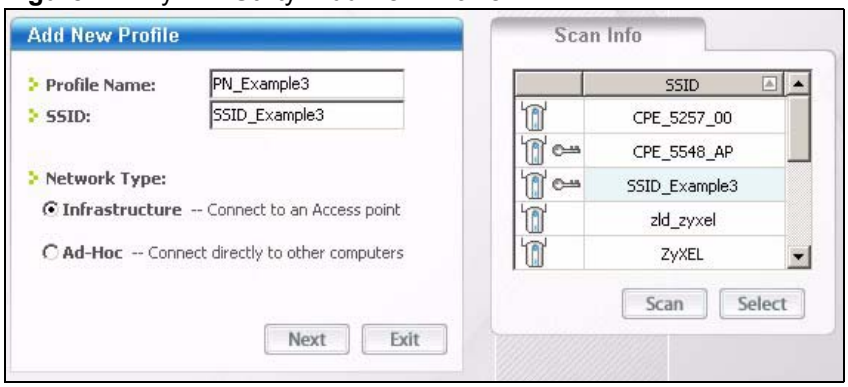
1 Open the ZyXEL utility and click the **Profile** tab to open the screen as shown. Click **Add** to configure a new profile.

**Figure 13** ZyXEL Utility: Profile




2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. You can also configure your profile for a wireless network that is not in the list.

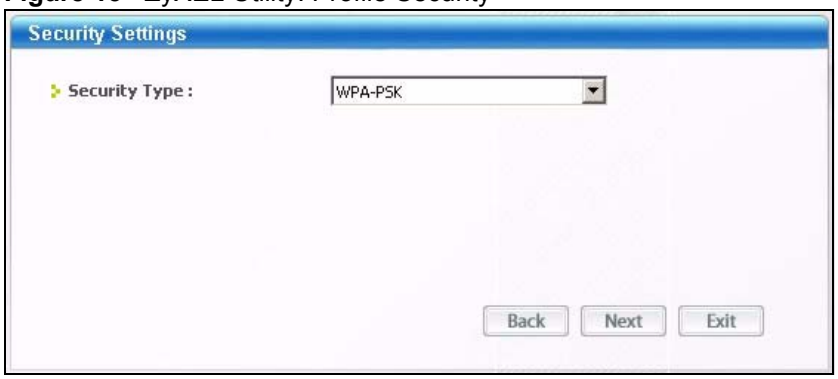
**Figure 14** ZyXEL Utility: Add New Profile




3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

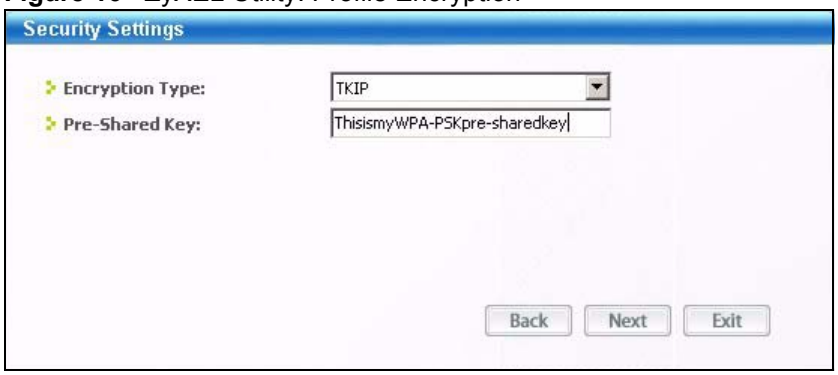
4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

**Figure 15** ZyXEL Utility: Profile Security



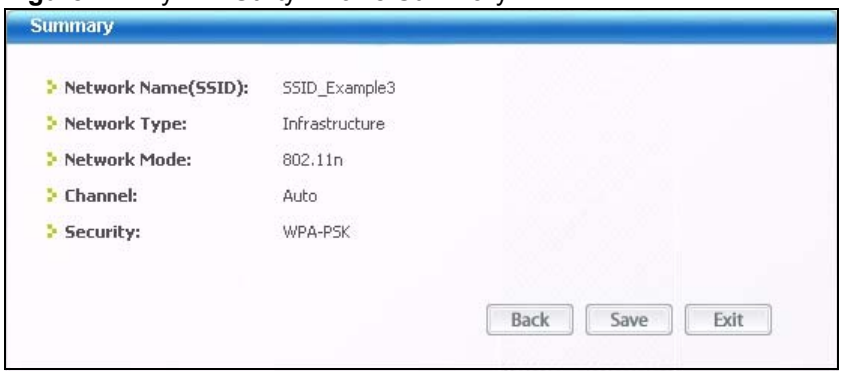

5 This screen varies depending on the encryption method you selected in the previous screen. In this example, enter the pre-shared key and leave the encryption type at the default setting.

**Figure 16** ZyXEL Utility: Profile Encryption




6 Verify the profile settings in the ready-only screen. Click **Save** to save and go to the next screen.

**Figure 17** ZyXEL Utility: Profile Summary




7 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button to go back to the **Profile List** screen.

If you clicked **Activate Later** you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Only one profile can be activated and used at any given time.

**Figure 18** ZyXEL Utility: Profile Activate

8 When you activate the new profile, the ZyXEL utility goes to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

9 Make sure the selected AP in the active profile is on and connected to the Internet. Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

10 If you cannot access the Internet, go back to the **Profile** screen. Select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

# 3

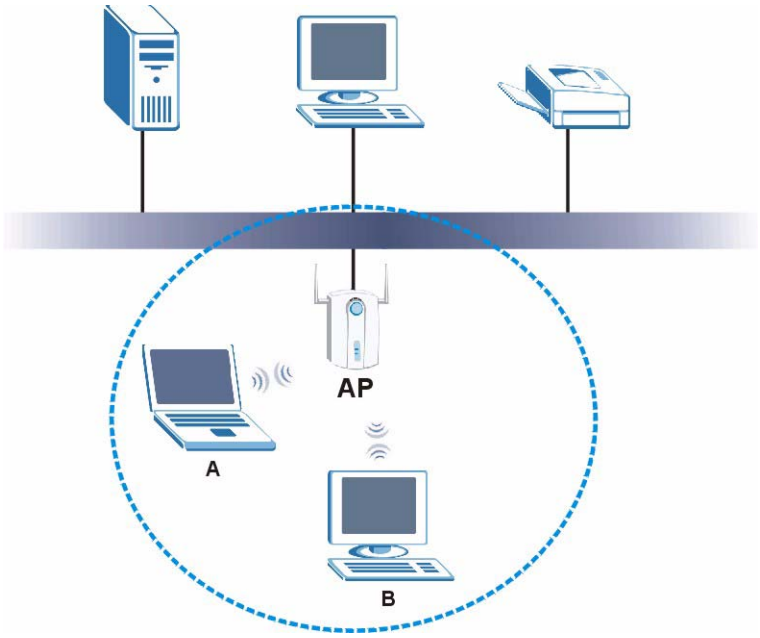
# Wireless LANs

This chapter provides background information on wireless Local Area Networks.

## 3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See Figure 3 on page 24 for an Ad Hoc network example.

**Figure 19** Example of a Wireless Network




The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP or peer computer.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## 3.2 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communications.

If you do not enable any wireless security on your NWD310N, the NWD310N's wireless communications are accessible to any wireless networking device that is in the coverage area.

You can use only WEP encryption if you set the NWD310N to Ad-hoc mode.

See the appendices for more detailed information about wireless security.

### 3.2.1 User Authentication and Encryption

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

#### 3.2.1.1 WEP

##### *3.2.1.1.1 Data Encryption*

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the NWD310N and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your NWD310N.

- Automatic WEP key generation based on a "password phrase" called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.

  For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the ZyXEL utility and entering them manually as the WEP keys in the other WLAN adapter(s).
- Enter the WEP keys manually.

Your NWD310N allows you to configure up to four 64-bit, 128-bit or 152-bit WEP keys. Only one key is used as the default key at any one time.

#### *3.2.1.1.2 Authentication Type*

The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Three authentication types are defined: **Auto**, **Open** and **Shared**.

- **Open** mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- **Shared** mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.
- **Auto** authentication mode allows the NWD310N to switch between the open system and shared key modes automatically. Use the auto mode if you do not know the authentication mode of the other wireless stations.

### 3.2.1.2 IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

#### *3.2.1.2.1 EAP Authentication*

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. The NWD310N supports EAP-TLS, EAP-TTLS (at the time of writing, TTLS is not available in Windows Vista) and EAP-PEAP. Refer to Appendix B on page 103 for descriptions.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). Certificates (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

### 3.2.1.3 WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## 3.3 WiFi Protected Setup

Your NWD310N supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

### 3.3.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the NWD310N, see Section 4.5.1 on page 62).
3. Press the button on one of the devices (it doesn't matter which).
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

### 3.3.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the NWD310N, see Section 4.5 on page 61).
4. Enter the client's PIN in the AP's configuration interface.

If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

5. Start WPS on both devices within two minutes.

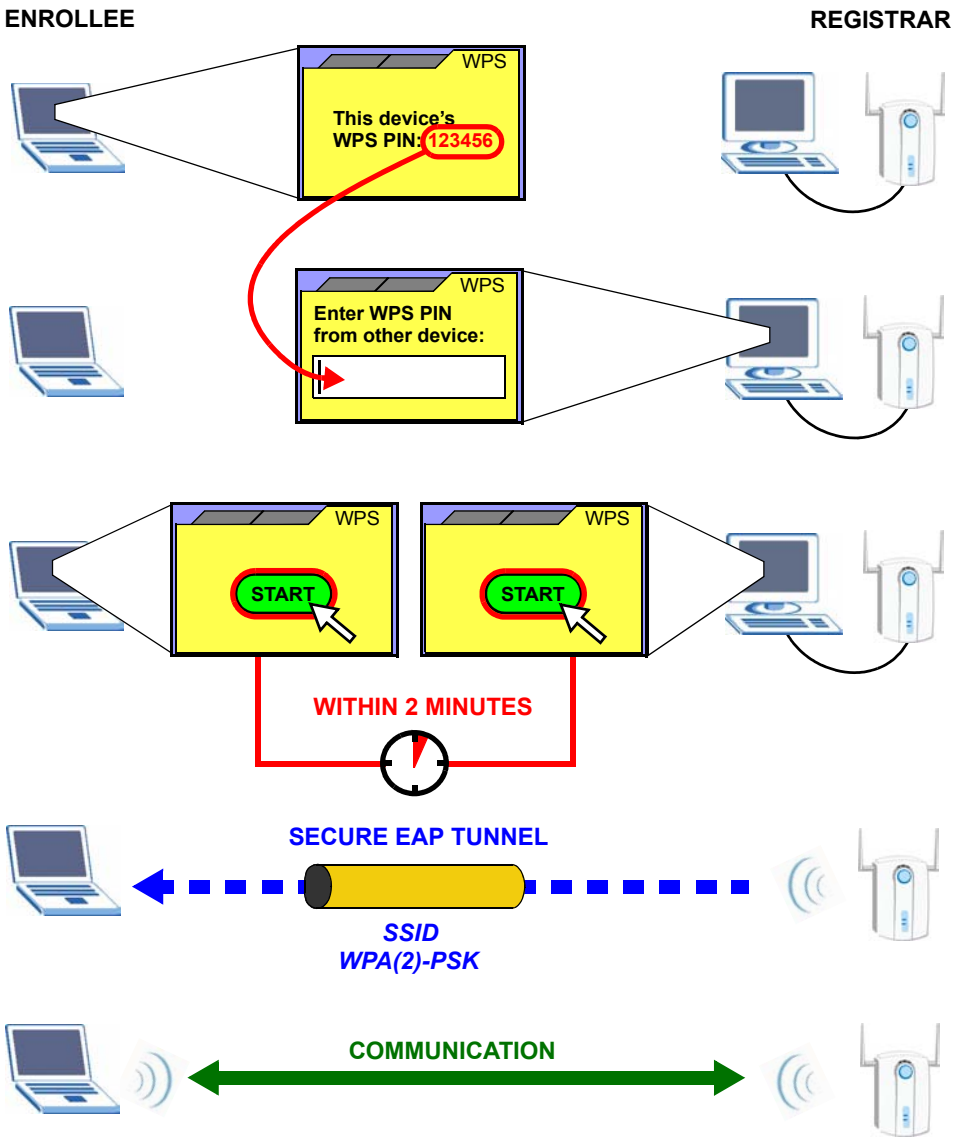
Use the configuration utility to activate WPS, not the push-button on the device itself.

6. On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

   If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

**Figure 20** Example WPS Process: PIN Method

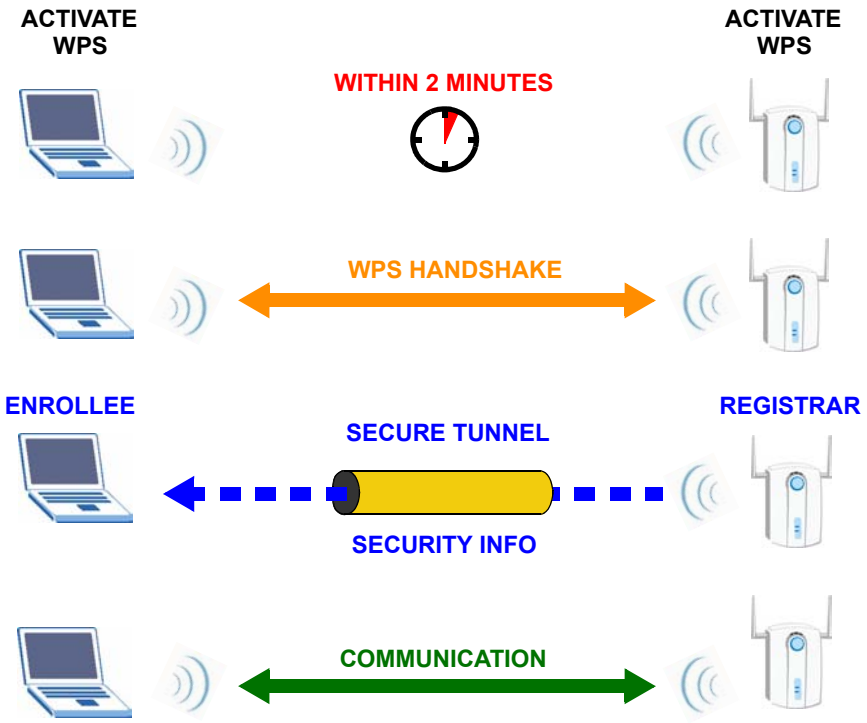



## 3.3.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

**Figure 21** How WPS works




The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

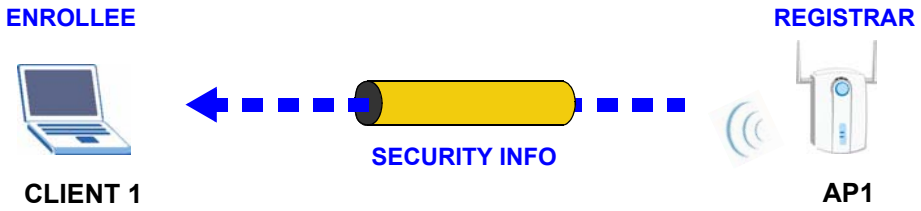
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

#### 3.3.3.1 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

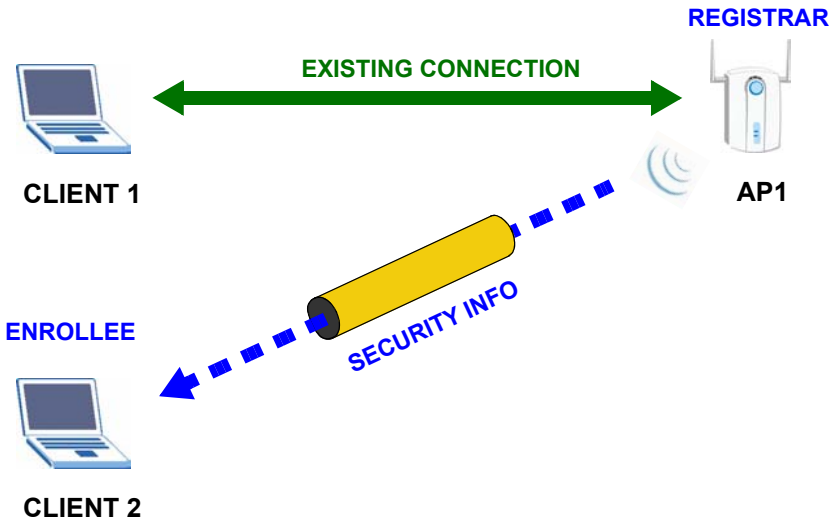
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 22** WPS: Example Network Step 1



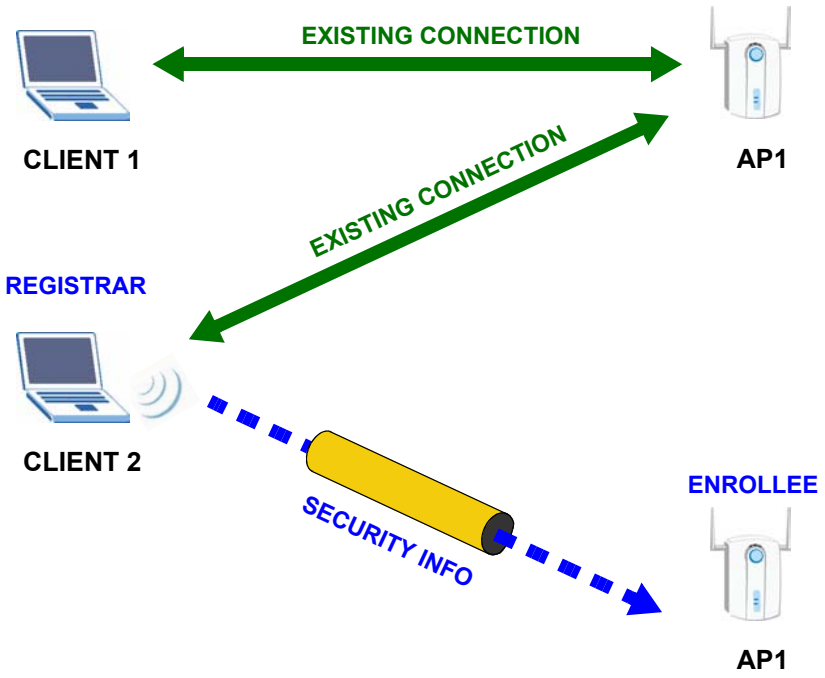

In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

**Figure 23** WPS: Example Network Step 2




In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

**Figure 24** WPS: Example Network Step 3




## 3.3.4 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices (see Section 4.3.1.2 on page 52 for information on pre-shared keys). Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

# 4

# Wireless Configuration

This chapter shows you how to configure your NWD310N.

## 4.1 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens.

**Figure 25** ZyXEL Utility Menu Summary

The following table describes the menus.

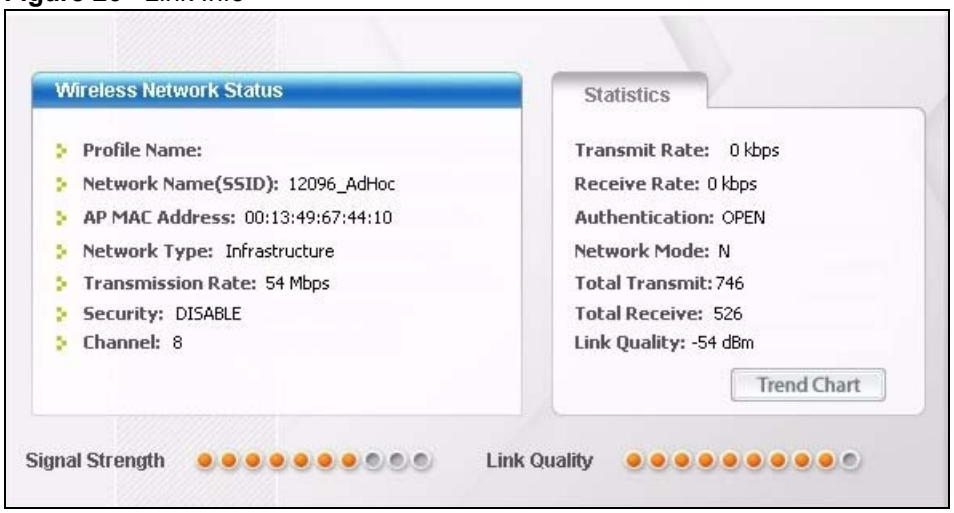
**Table 4** ZyXEL Utility Menu Summary

| TAB | DESCRIPTION |
|---|---|
| Link Info | Use this screen to see your current connection status, configuration and data rate statistics. |
| Site Survey | Use this screen to<br>• scan for a wireless network<br>• configure wireless security (if activated on the selected network).<br>• connect to a wireless network. |
| Profile | Use this screen to add, delete, edit or activate a profile with a set of wireless and security settings. |
| Adapter | Use this screen to configure preamble type, enable power saving and use WiFi Protected Setup (WPS). |

## 4.2 The Link Info Screen

When the ZyXEL utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your NWD310N.

**Figure 26** Link Info




The following table describes the labels in this screen.

**Table 5** Link Info

| LABEL | DESCRIPTION |
|---|---|
| Wireless Network Status | |
| Profile Name | This is the name of the profile you are currently using. |
| Network Name (SSID) | The SSID identifies the wireless network to which a wireless station is associated. This field displays the name of the wireless device to which the NWD310N is associated. |
| AP MAC Address | This field displays the MAC address of the AP or peer computer to which the NWD310N is associated. |
| Network Type | This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless network. |
| Transmission Rate | This field displays the current transmission rate of the NWD310N in megabits per second (Mbps). |
| Security | This field displays whether data encryption is activated (**WEP** / **802.1x** / **WPA** / **WPA-PSK** / **WPA2** / **WPA2-PSK**) or inactive (**DISABLE**). |
| Channel | This field displays the radio channel the NWD310N is currently using. |
| Statistics | |
| Transmit Rate | This field displays the current data transmission rate in kilobits per second (Kbps). |
| Receive Rate | This field displays the current data receiving rate in kilobits per second (Kbps). |
| Authentication | This field displays the authentication method of the NWD310N. |
| Network Mode | This field displays the wireless standard (**802.11b**, **802.11g** or **802.11n**) of the AP or peer computer. |
| Total Transmit | This field displays the total number of data frames transmitted. |
| Total Receive | This field displays the total number of data frames received. |
| Link Quality | This field displays the signal strength of the NWD310N. |
| Trend Chart | Click this button to display the real-time statistics of the data rate in kilobits per second (Kbps). |

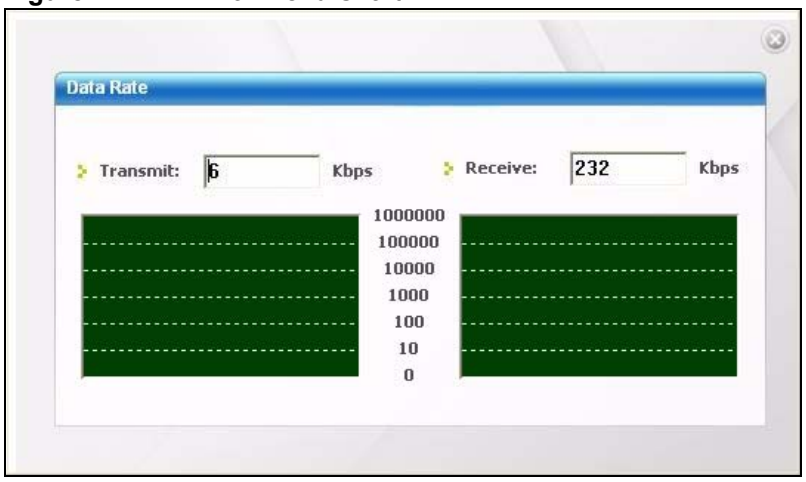
**Table 5** Link Info (continued)

| LABEL | DESCRIPTION |
|---|---|
| Signal Strength | The status bar shows the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your NWD310N and the AP or peer computer. |
| Link Quality | The status bar shows the quality of wireless connection. This refers to the percentage of packets transmitted successfully. If there are too many wireless stations in a wireless network, collisions may occur which could result in a loss of messages even though you have high signal strength. |

### 4.2.1 Trend Chart

Click **Trend Chart** in the **Link Info** screen to display a screen as shown below. Use this screen to view real-time data traffic statistics.

**Figure 27** Link Info: Trend Chart




The following table describes the labels in this screen.

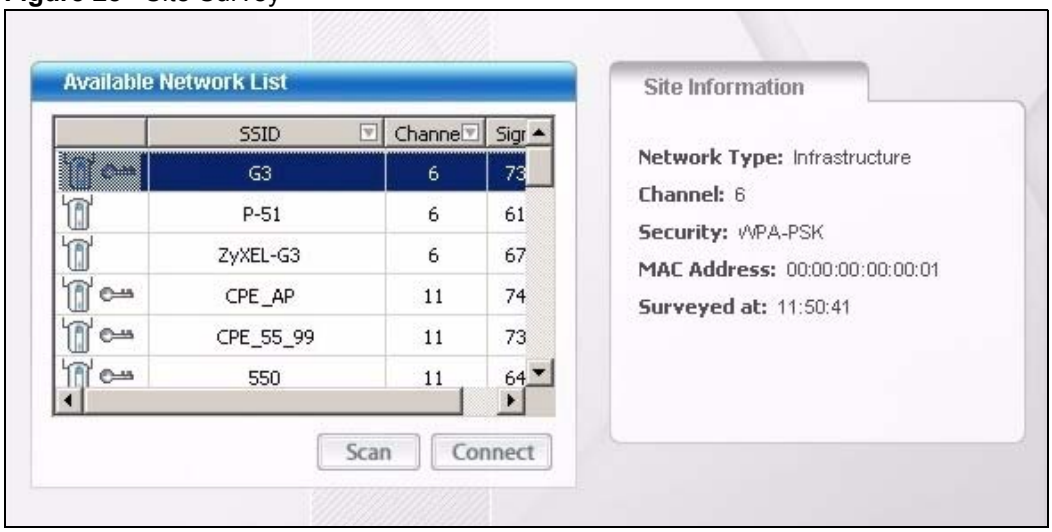
**Table 6** Link Info: Trend Chart

| LABEL | DESCRIPTION |
|---|---|
| Transmit | This field displays the current data transmission rate in kilobits per second (Kbps). |
| Receive | This field displays the current data reception rate in kilobits per second (Kbps). |

## 4.3 The Site Survey Screen

Use the **Site Survey** screen to scan for and connect to a wireless network automatically.

**Figure 28** Site Survey




The following table describes the labels in this screen.

**Table 7** Site Survey

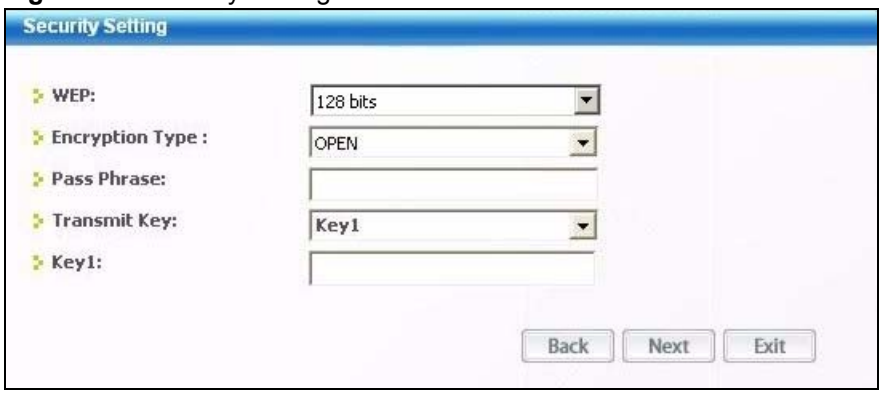
| LABEL | DESCRIPTION |
|---|---|
| Available Network List | Click a column heading to sort the entries. |
| , , or | denotes that the wireless device is in infrastructure mode and the wireless security is activated.<br>denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.<br>denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.<br>denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated. |
| SSID | This field displays the SSID (Service Set IDentifier) of each wireless device. |
| Channel | This field displays the channel number used by each wireless device. |
| Signal | This field displays the signal strength of each wireless device. |
| Scan | Click **Scan** to search for available wireless devices within transmission range. |
| Connect | Click **Connect** to associate to the selected wireless device. |
| Site Information | Click an entry in the **Available Network List** table to display the information of the selected wireless device. |
| Network Type | This field displays the network type (**Infrastructure** or **Ad Hoc**) of the wireless device. |
| Network Mode | This field displays the wireless standard (**802.11b**, **802.11g** or **802.11n**) used by the selected wireless device. |
| Channel | This field displays the channel number used by each wireless device. |
| Security | This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK** or **802.1x**) or inactive (**DISABLE**). |
| MAC address | This field displays the MAC address of the wireless device. |
| Surveyed at | This field displays the time when the wireless device was scanned. |

## 4.3.1 Security Settings

When you configure the NWD310N to connect to a network with wireless security activated and the security settings are disabled on the NWD310N, the screen varies according to the encryption method used by the selected network.

### 4.3.1.1 WEP Encryption

**Figure 29** Security Setting: WEP




The following table describes the labels in this screen.

**Table 8** Security Setting: WEP

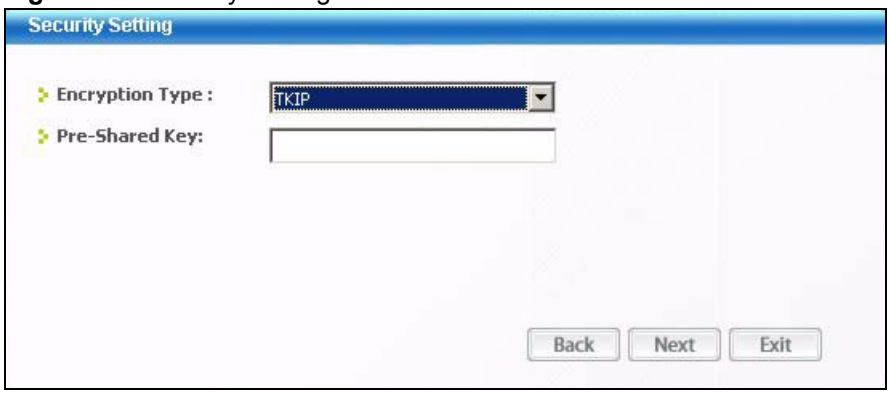
| LABEL | DESCRIPTION |
|---|---|
| Security Settings | |
| WEP | Select **64 Bits** or **128 Bits** to activate WEP encryption and then fill in the related fields. |
| Encryption Type | Select an authentication method. Choices are **Open** and **Shared**.<br>Refer to Section 3.2.1.1.2 on page 39 for more information. |
| Pass Phrase | Enter a passphrase of up to 32 case-sensitive printable characters. As you enter the passphrase, the NWD310N automatically generates four different WEP keys and displays the first in the key field below. Refer to Section 3.2.1.1.1 on page 38 for more information. |
| Transmit Key | Select a default WEP key to use for data encryption. The key displays in the adjacent field. |
| Key x (where x is a number between 1 and 4) | Select this option if you want to manually enter the WEP keys. Enter the WEP key in the field provided.<br>If you select **64 Bits** in the **WEP** field.<br>Enter either 10 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 11AA22BB33) for HEX key type.<br>or<br>Enter 5 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey) for ASCII key type.<br>If you select **128 Bits** in the **WEP** field,<br>Enter either 26 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 00112233445566778899AABBCC) for HEX key type<br>or<br>Enter 13 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey12345678) for ASCII key type.<br>Note: The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. ASCII WEP keys are case sensitive. |

**Table 8** Security Setting: WEP (continued)

| LABEL | DESCRIPTION |
|---|---|
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Next | Click **Next** to confirm your selections and advance to the **Summary** screen. Refer to Section 4.3.3 on page 55. |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

### 4.3.1.2 WPA-PSK/WPA2-PSK

**Figure 30** Security Setting: WPA-PSK/WPA2-PSK




The following table describes the labels in this screen.

**Table 9** Security Setting: WPA-PSK/WPA2-PSK

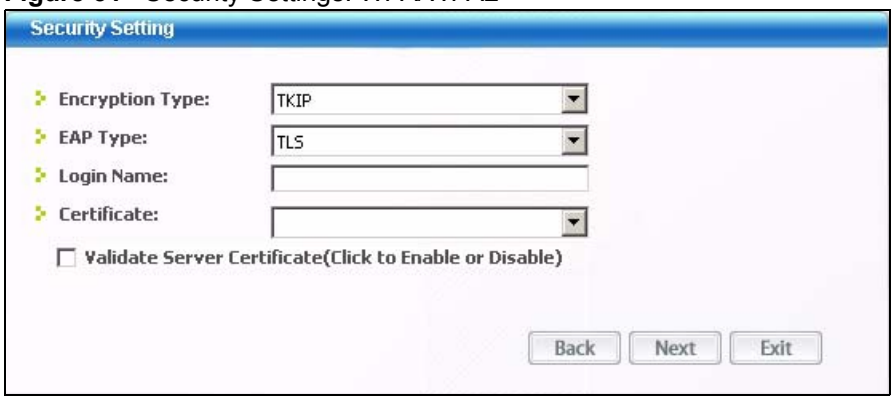
| LABEL | DESCRIPTION |
|---|---|
| Encryption Type | The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials.<br>Select the encryption type (**TKIP** or **AES**) for data encryption.<br>Refer to Section 3.2.1.3 on page 39 for more information. |
| Pre-Shared Key | Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters. |
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Next | Click **Next** to confirm your selections and advance to the **Summary** screen. Refer to Section 4.3.3 on page 55. |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

### 4.3.1.3 WPA/WPA2

The screen that displays when you select **WPA** or **WPA2** differs, depending on the **EAP Type** you select (**TLS**, **PEAP** or **TTLS**).

The procedure to configure WPA or WPA2 is different in Windows Vista. See Section 4.6 on page 64 for information on setting up your NWD310N to use WPA or WPA2 in Vista.

**Figure 31** Security Settings: WPA/WPA2




The following table describes the labels in this screen.

**Table 10** Security Setting: WPA/WPA2

| LABEL | DESCRIPTION |
|---|---|
| Encryption Type | The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials.<br>Select the encryption type (**TKIP** or **AES**) for data encryption.<br>Refer to Section 3.2.1.3 on page 39 for more information. |
| EAP Type | The type of authentication you use depends on the RADIUS server or AP.<br>Select an authentication method from the drop down list. Options are **TLS**, **PEAP** and **TTLS** (at the time of writing, TTLS is not available in Windows Vista). |
| Login Name | Enter a user name.<br>This is the user name that you or an administrator set up on a RADIUS server. |
| Password | This field is not available when you select **TLS** in the **EAP Type** field.<br>Enter the password associated with the user name above. |
| Certificate | This field is only available when you select **TLS** in the **EAP Type** field.<br>Click **Browse** to select a certificate.<br><br>Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information. |
| Validate Server Certificate | Select this to verify the certificate of the authentication server.<br>If you select this and click **Next**, the **Server Certificate Setting** screen displays. |
| PEAP Inner EAP | This field is only available when you select **PEAP** in the **EAP Type** field.<br>The PEAP method used by the RADIUS server or AP for client authentication is **MS CHAP v2**. |
| TTLS Protocol | This field is available only when you select **TTLS** in the **EAP Type** field.<br>Select a TTLS protocol that the RADIUS server uses. Options are **CHAP**, **MS-CHAP**, **MS-CHAP-V2** and **PAP**. |
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Next | Click **Next** to confirm your selections and advance to the **Summary** screen (refer to Section 4.3.3 on page 55.)<br>If you selected **Validate Server Certificate**, the **Server Certificate Setting** screen displays (refer to Section 4.3.2 on page 55). |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

#### 4.3.1.4 IEEE 802.1x

Configure IEEE 802.1x security with various authentication methods in this screen.

The procedure to configure 802.1x is different in Windows Vista. See Section 4.6 on page 64 for information on setting up your NWD310N to use 802.1x in Vista.

**Figure 32** Security Setting: 802.1x

The following table describes the labels in this screen.

**Table 11** Security Settings: IEEE 802.1x

| LABEL | DESCRIPTION |
|---|---|
| Encryption Type | Select **WEP** if the access point is configured to use 802.1x with WEP encryption. A dynamic WEP key is generated automatically.<br>Otherwise, select **Disable** (at the time of writing, this is not available in Windows Vista). |
| EAP Type | The type of authentication you use depends on the RADIUS server or AP.<br>Select an authentication method from the drop down list. Options are **TLS**, **PEAP** and **TTLS** (at the time of writing, TTLS is not available in Windows Vista). |
| Login Name | Enter a user name.<br>This is the user name that you or an administrator set up on a RADIUS server. |
| Password | This field is not available when you select **TLS** in the **EAP Type** field.<br>Enter the password associated with the user name above. |
| Certificate | This field is only available when you select **TLS** in the **EAP Type** field.<br>Click **Browse** to select a certificate.<br><br>Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information. |
| Validate Server Certificate | Select this to verify the certificate of the authentication server.<br>If you select this and click **Next**, the **Server Certificate Setting** screen displays. |
| PEAP Inner EAP | This field is only available when you select **PEAP** in the **EAP Type** field.<br>The PEAP method used by the RADIUS server or AP for client authentication is **MS CHAP v2**. |

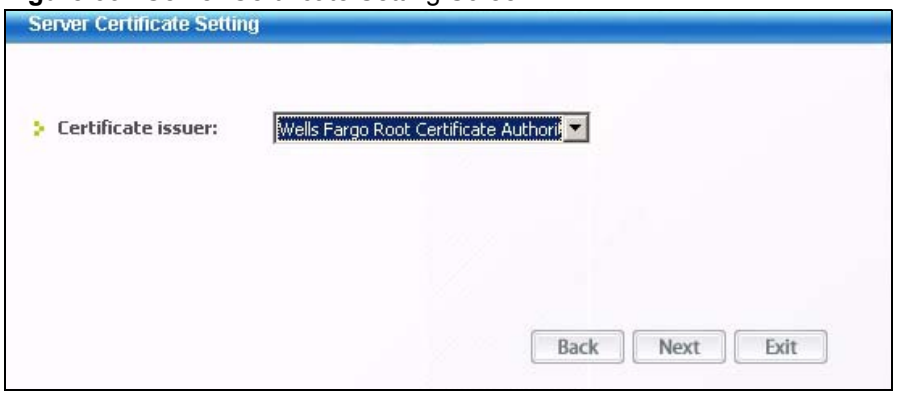
**Table 11** Security Settings: IEEE 802.1x

| LABEL | DESCRIPTION |
|---|---|
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Next | Click **Next** to confirm your selections and advance to the **Summary** screen (refer to Section 4.3.3 on page 55.)<br>If you selected **Validate Server Certificate**, the **Server Certificate Setting** screen displays (refer to Section 4.3.2 on page 55). |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

## 4.3.2 Server Certificate Setting Screen

This screen displays if you selected **Validate Server Certificate** in the **WPA**, **WPA2** or **802.1x** screens.

**Figure 33** Server Certificate Setting Screen




The following table describes the labels in this screen.

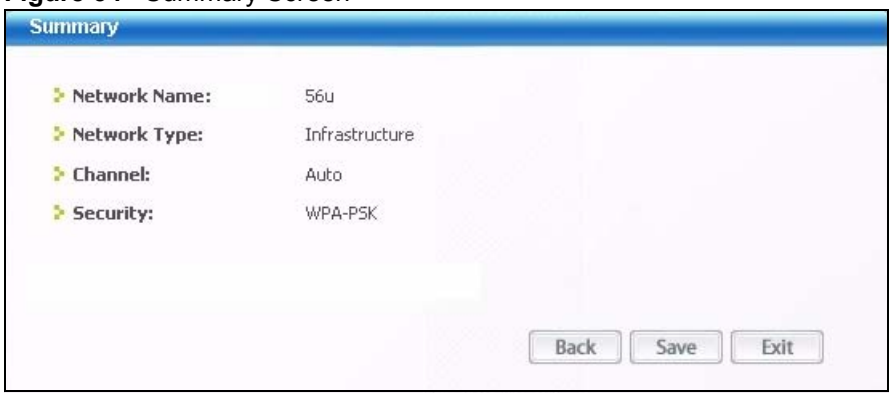
**Table 12** Server Certificate Setting

| LABEL | DESCRIPTION |
|---|---|
| Certificate Issuer | Select the name of the certificate authority from the list. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue to the **Summary** screen. |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

## 4.3.3 Summary Screen

Use this screen to confirm and save the security settings.

**Figure 34** Summary Screen




The following table describes the labels in this screen.

**Table 13** Summary Screen

| LABEL | DESCRIPTION |
|---|---|
| Network Name (SSID) | This field displays the SSID previously entered. |
| Network Type | This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless device. |
| Channel | This field displays the channel number used by the profile. |
| Security | This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**, **802.1x**) or inactive (**DISABLE**). |
| Back | Click **Back** to return to the previous screen. |
| Save | Click **Save** to save the changes back to the NWD310N and display the **Link Info** screen. |
| Exit | Click **Exit** to discard changes and return to the **Site Survey** screen. |

## 4.4 The Profile Screen

A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the NWD310N, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available, the NWD310N cannot connect to a network.

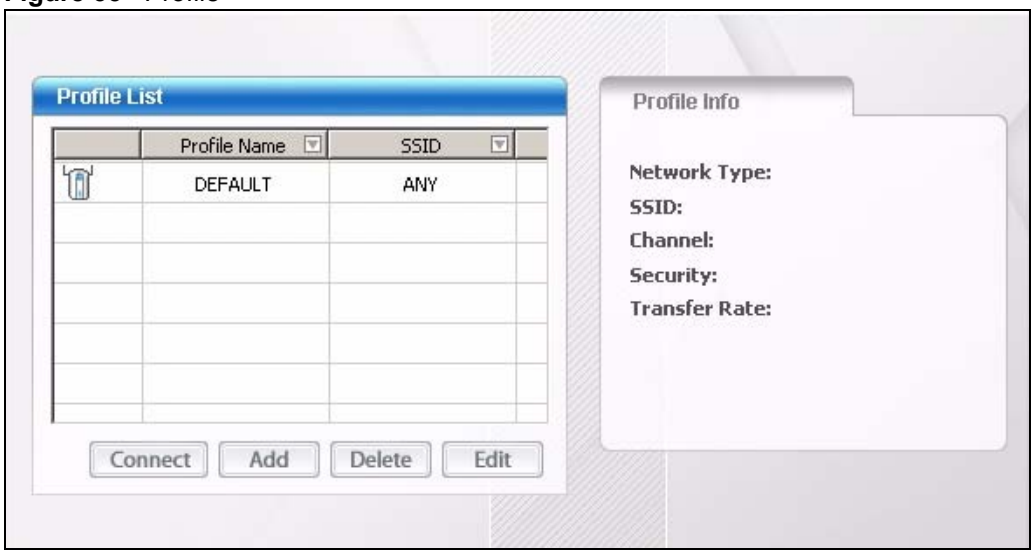
If you do not configure and activate a profile, each time you start the NWD310N, the NWD310N uses the default profile to connect to any available network that has no security enabled.

The default profile is a profile that allows you to connect to any SSID that has no security enabled.

Click the **Profile** tab in the ZyXEL utility program to display the **Profile** screen as shown next.

The profile function allows you to save the wireless network settings in this screen, or use one of the pre-configured network profiles.

**Figure 35** Profile




The following table describes the labels in this screen.

**Table 14** Profile

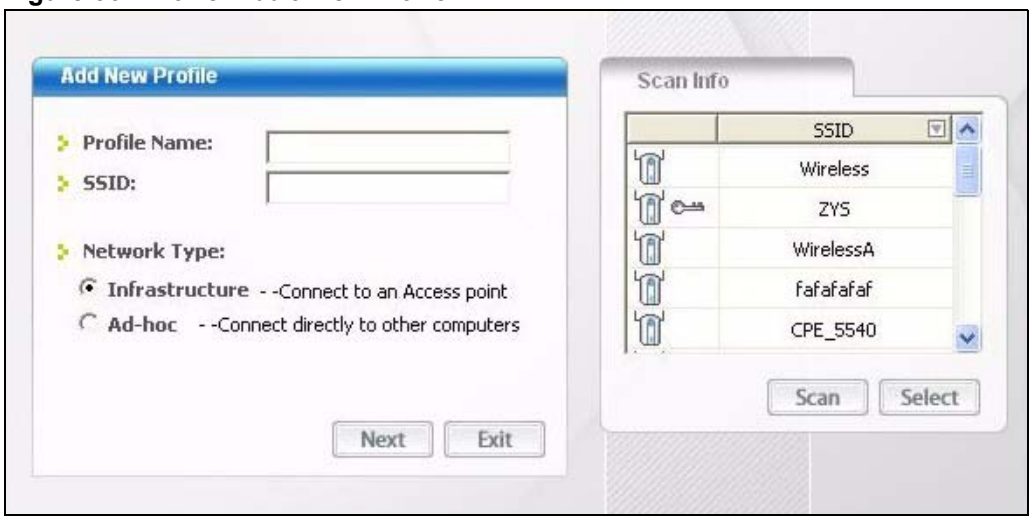
| LABEL | DESCRIPTION |
|---|---|
| Profile List | Click a column heading to sort the entries. |
| , , or | denotes that the wireless device is in infrastructure mode and the wireless security is activated.<br>denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.<br>denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.<br>denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated. |
| Profile Name | This is the name of the pre-configured profile. |
| SSID | This is the SSID of the wireless network to which the selected profile associate. |
| Connect | To use and activate a previously saved network profile, select a pre-configured profile name in the table and click **Connect**. |
| Add | To add a new profile into the table, click **Add**. |
| Delete | To delete an existing wireless network configuration, select a profile in the table and click **Delete**. |
| Edit | To edit an existing wireless network configuration, select a profile in the table and click **Edit**. |
| Profile Info | The following fields display detailed information of the selected profile in the **Profile List** table. |
| Network Type | This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the profile. |
| SSID | This field displays the network's Service Set IDentity (the name of the network). |
| Channel | This field displays the channel number used by the profile. |
| Security | This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK** or **802.1x**) or inactive (**DISABLE**). |
| Transfer Rate | This field displays the transmission speed of the selected profile in megabits per second (Mbps). |

### 4.4.1 Adding a New Profile

Follow the steps below to add a new profile.

1 Click **Add** in the **Profile** screen. An **Add New Profile** screen displays as shown next.

**Figure 36** Profile: Add a New Profile




The following table describes the labels in this screen.

**Table 15** Profile: Add a New Profile

| LABEL | DESCRIPTION |
|---|---|
| Add New Profile | |
| Profile Name | Enter a descriptive name in this field. |
| SSID | Select an available wireless device in the **Scan Info** table and click **Select**, or enter the SSID of the wireless device to which you want to associate in this field manually. Otherwise, enter **Any** to have the NWD310N associate to any AP or roam between any infrastructure wireless networks. |
| Network Type | Select **Infrastructure** to associate to an AP. Select **Ad-Hoc** to associate to a peer computer. |
| Next | Click **Next** to go to the next screen. |
| Exit | Click **Exit** to go back to the previous screen without saving. |
| Scan Info | This table displays the information of the available wireless networks within the transmission range. |
| , , or | denotes that the wireless device is in infrastructure mode and the wireless security is activated.<br>denotes that the wireless device is in infrastructure mode but the wireless security is deactivated.<br>denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated.<br>denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated. |
| SSID | This field displays the SSID (Service Set IDentifier) of each AP or peer device. |

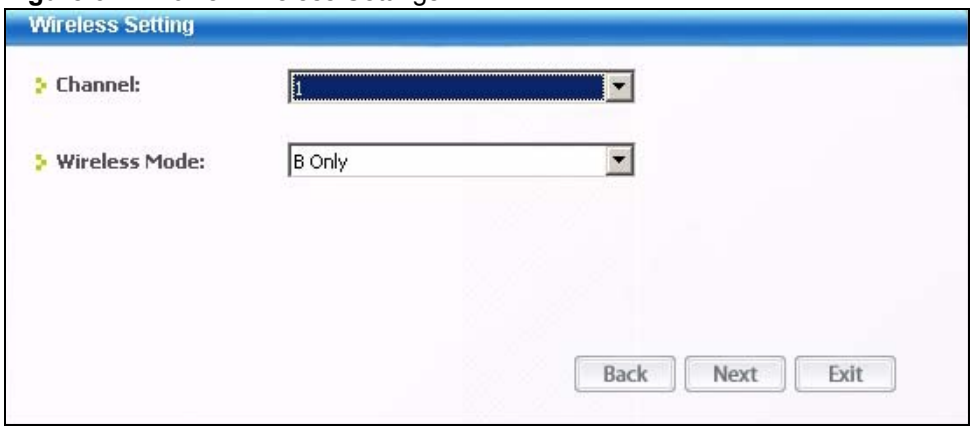
**Table 15** Profile: Add a New Profile (continued)

| LABEL | DESCRIPTION |
|---|---|
| Scan | Click **Scan** to search for available wireless devices within transmission range. |
| Select | Select an available wireless device in the table and click **Select** to add it to this profile.<br>Whenever you activate this profile, the NWD310N associates to the selected wireless network only. |

**2** If you select the **Infrastructure** network type in the previous screen, skip to step 3. If you select the **Ad-Hoc** network type in the previous screen, a screen displays as follows. Select a **Channel** number and **Wireless Mode** and click **Next** to continue.

To associate to an ad-hoc network, you must use the same channel as the peer computer.

**Figure 37** Profile: Wireless Settings



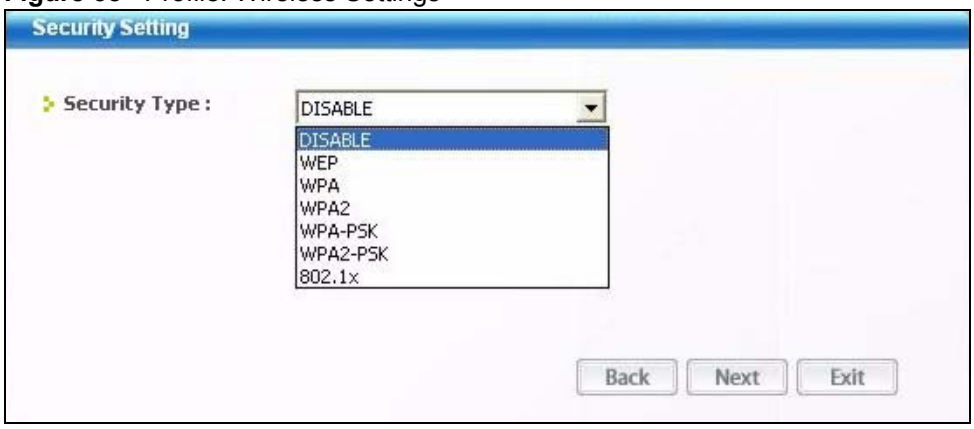

The following table describes the labels in this screen.

**Table 16** Profile: Wireless Settings

| LABEL | DESCRIPTION |
|---|---|
| Wireless Settings | |
| Channel | Select a channel number from the drop-down list box. To associate to an ad-hoc network, you must use the same channel as the peer computer. |
| Wireless Mode | This is the wireless standard the NWD310N uses. In Ad-Hoc mode, you can use only 802.11b or 802.11g. |

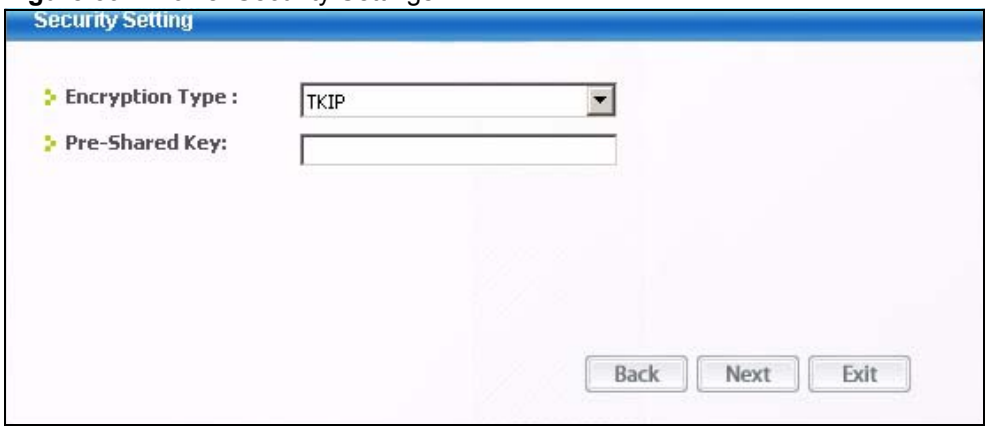
**3** If you selected **Infrastructure** network type in the first screen, select **WEP**, **WPA**, **WPA2**, **WPA-PSK**, **WPA2-PSK** or **802.1x** from the drop-down list box to enable data encryption. If you selected **Ad-Hoc** network type in the first screen, you can use only **WEP** encryption method. Otherwise, select **DISABLE** to allow the NWD310N to communicate with the access points or other peer wireless computers without any data encryption, and skip to step 5.

**Figure 38** Profile: Wireless Settings



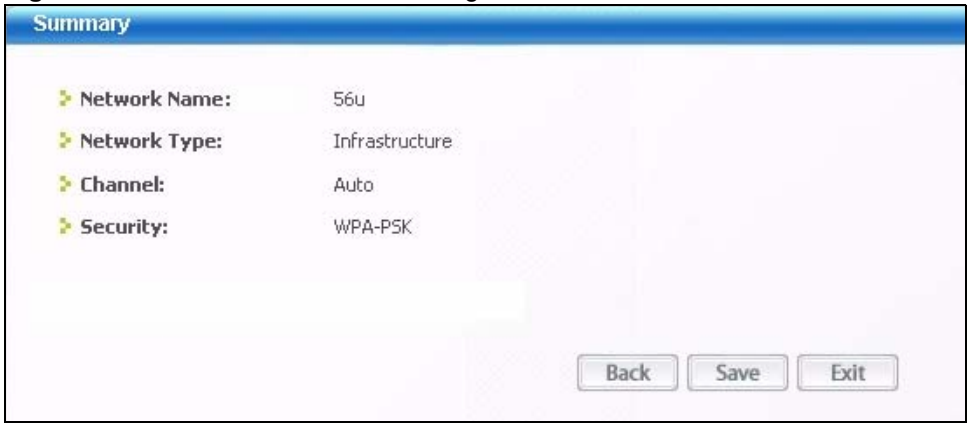

**4** The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the AP or other peer wireless computers as they are on the NWD310N. Refer to Section 4.3.1 on page 51 for detailed information on wireless security configuration.

**Figure 39** Profile: Security Settings




**5** This read-only screen shows a summary of the new profile settings. Verify that the settings are correct. Click **Save** to save and go to the next screen. Click **Back** to return to the previous screen. Otherwise, click **Exit** to go back to the **Profile** screen without saving.

**Figure 40** Profile: Confirm New Settings



6 To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button. You can activate only one profile at a time.

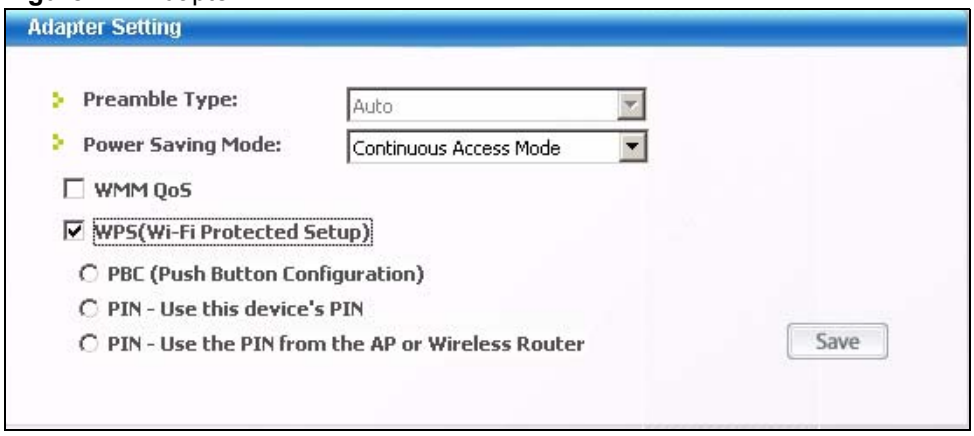
Once you activate a profile, the ZyXEL utility will use that profile the next time it is started.

**Figure 41** Profile: Activate the Profile

## 4.5 The Adapter Screen

To set the other advanced features on the NWD310N, click the **Adapter** tab.

**Figure 42** Adapter




The following table describes the labels in this screen.

**Table 17** Adapter

| LABEL | DESCRIPTION |
|---|---|
| Adapter Setting | |
| Preamble Type | Preamble is used to signal that data is coming to the receiver. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.<br>The NWD310N automatically uses short preamble when the access point supports it; otherwise the NWD310N uses long preamble.<br>At the time of writing, this field is not available in Windows Vista. |

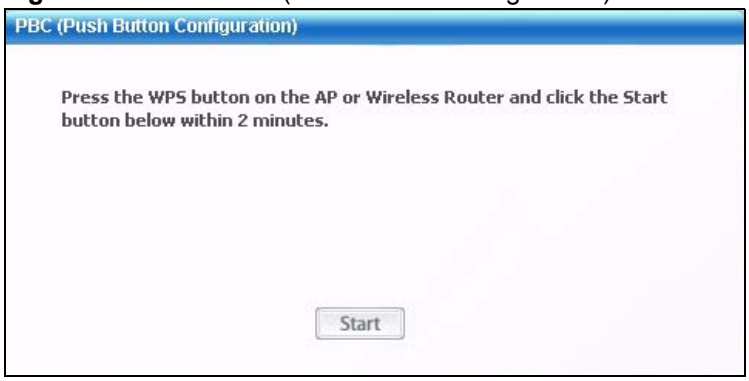
**Table 17** Adapter (continued)

| LABEL | DESCRIPTION |
|---|---|
| Power Saving Mode | Select **Fast Power Save** to save power. This forces the NWD310N to go to sleep mode when it is not transmitting data.<br>When you select **Continuous Access Mode**, the NWD310N will never go to sleep mode.<br>At the time of writing, this field is not available in Windows Vista. |
| WMM QoS | Select this to enable Wi-fi MultiMedia Quality of Service on the NWD310N.<br>At the time of writing, this field is not available in Windows Vista. |
| WPS (WiFi Protected Setup) | Select this to enable Wi-fi Protected Setup on the NWD310N. |
| PBC (Push Button Configuration) | Select this to use the PBC (Push-Button Configuration) WPS mode. When you use the PBC mode you do not use a PIN.<br>When you select this, the **PBC (Push Button Configuration** screen appears (see Section 4.5.1 on page 62). |
| PIN - Use This Device's PIN | Select this to use the PIN (Personal Identification Number) WPS mode. Use this option when you want to enter the NWD310N's PIN in another WPS-enabled device.<br>When you select this, the **PIN - Use this Device's PIN** screen appears (see Section 4.5.2 on page 63). |
| PIN - Use the PIN From the AP or Wireless Router | Select this to use the PIN (Personal Identification Number) WPS mode. Use this option when you want to enter the PIN from another WPS-enabled device in the NWD310N.<br>When you select this, the **PIN - Use the PIN From the AP or Wireless Router** screen appears (see Section 4.5.3 on page 63). |
| Save | Click **Save** to save the changes to the NWD310N and return to the **Link Info** screen. |

## 4.5.1 WPS: PBC (Push Button Configuration)

This screen allows you to use the WPS Push Button Configuration mode. See Section 3.3.1 on page 40 for more information. Select **WPS** and **PBC (Push Button Configuration)** in the **Adapter** screen. The following screen displays.

**Figure 43** WPS: PBC (Push Button Configuration)

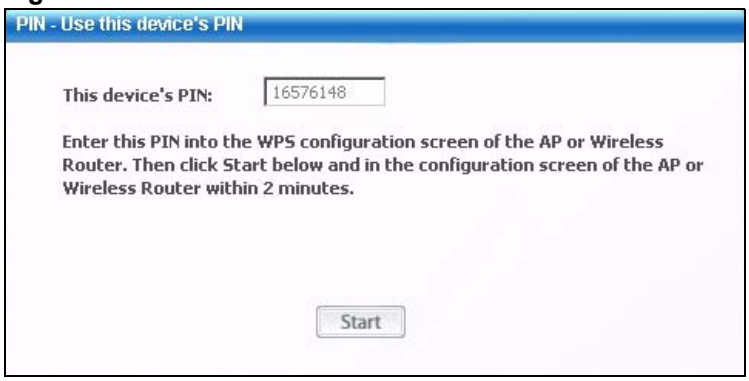

PBC (Push Button Configuration)
Press the WPS button on the AP or Wireless Router and click the Start button below within 2 minutes.
Start

Press **Start** when you want to begin the WPS process. You must also press the button on the other device within two minutes.

## 4.5.2 WPS: PIN - Use this Device's PIN

This screen allows you to use the WPS Personal Identification Number mode, by entering the NWD310N's unique PIN in the configuration utility of the other WPS-enabled device. See Section 3.3.2 on page 41 for more information. Select **WPS** and **PIN - Use this Device's PIN** in the **Adapter** screen. The following screen displays.

**Figure 44** WPS: PIN - Use this Device's PIN


PIN - Use this device's PIN
This device's PIN:
16576148
Enter this PIN into the WPS configuration screen of the AP or Wireless Router. Then click Start below and in the configuration screen of the AP or Wireless Router within 2 minutes.
Start

The following table describes the labels in this screen.

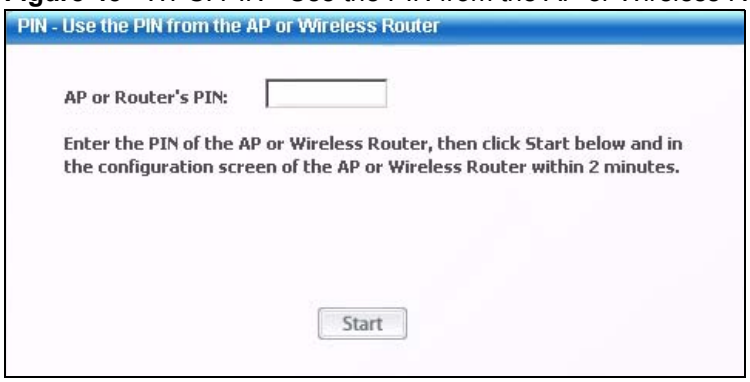
**Table 18** WPS: PIN - Use this Device's PIN

| LABEL | DESCRIPTION |
|---|---|
| This device's PIN | This is the NWD310N's Personal Identification Number (PIN). This field is read-only. Enter the number that displays in this field into the configuration interface of the other WPS-enabled device.<br><br>Note: Each time this screen displays, the PIN is different. The PIN is valid for only one WPS transaction. |
| Start | Click this to start WPS. You must start WPS on the other WPS-enabled device within two minutes. |

## 4.5.3 WPS: PIN - Use the PIN from the AP or Wireless Router

This screen allows you to use the WPS Personal Identification Number mode, by entering the PIN from another WPS-enabled device into the NWD310N's utility. See Section 3.3.2 on page 41 for more information. Select **WPS** and **PIN - Use the PIN from the AP or Wireless Router** in the **Adapter** screen. The following screen displays.

**Figure 45** WPS: PIN - Use the PIN from the AP or Wireless Router


PIN - Use the PIN from the AP or Wireless Router
AP or Router's PIN:
Enter the PIN of the AP or Wireless Router, then click Start below and in the configuration screen of the AP or Wireless Router within 2 minutes.
Start

The following table describes the labels in this screen.

**Table 19** WPS: PIN - Use the PIN from the AP or Wireless Router

| LABEL | DESCRIPTION |
|---|---|
| AP or Router's PIN | Enter the PIN from your AP or wireless router in this field before you click **Start**. |
| Start | Click this to start WPS. You must start WPS on the other WPS-enabled device within two minutes. |

## 4.6 Security Settings in Windows Vista

When you use the NWD310N in Windows Vista, the procedure for setting up WPA, WPA2 and 802.1x security settings is different from that of other operating systems (other security types are not affected).

The procedures for setting up WPA, WPA2 or 802.1x in Vista are the same. However, the procedure differs depending on whether you use PEAP (Protected Extensible Authentication Protocol) or TLS (Transport Layer Security) encryption. Consult your network administrator if you are unsure which type of encryption to use.

See section Section 4.6.1 on page 64 to use PEAP, or see section Section 4.6.2 on page 65 to use TLS.

TTLS (Tunneled TLS) is not available when using Windows Vista, at the time of writing.

### 4.6.1 Using PEAP in Vista

Take the following steps to set up WPA, WPA2 or 802.1x security using PEAP in Windows Vista.

1 Either select the AP to which you want to connect in the **Site Survey** screen (see Section 4.3 on page 49), or configure a profile in the normal way (see Section 4.4 on page 56).

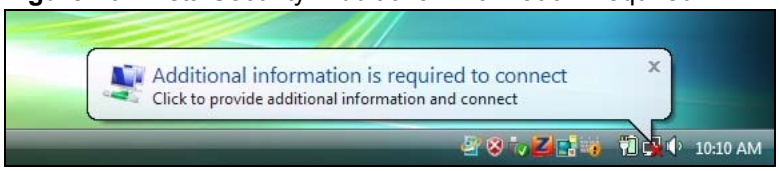
2 In the **WPA**, **WPA2** or **802.1x** security screen (see Section 4.3.1.3 on page 52 and Section 4.3.1.4 on page 54), select **PEAP** as the **EAP Type**. Note that the **Login Name** and **Password** fields are greyed-out (not available).

3 Click **Next**.

4 In the **Summary** screen that appears, click **Save**.

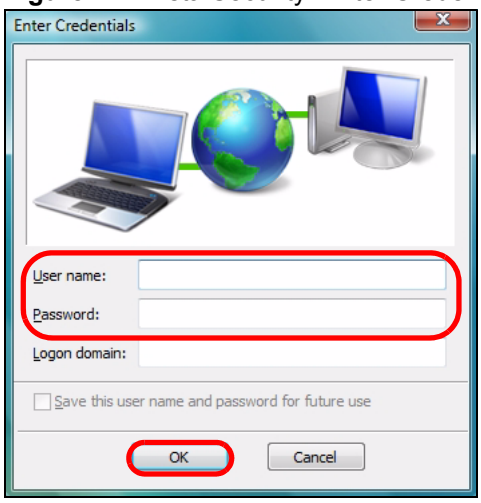
5 A message similar to the following appears in the bottom-right of your screen. Click the message.

**Figure 46** Vista Security: Additional Information Required




6 The **Enter Credentials** screen displays. Enter your **User name** and **Password** for the network to which you want to connect.

**Figure 47** Vista Security: Enter Credentials




If you are not sure what to enter, contact your network administrator.

7 Click **OK**. The **Enter Credentials** screen disappears and the NWD310N tries to connect to the network. The ZyXEL utility's **Link Info** screen displays, showing the connection status (see Section 4.2 on page 47). If the **Link Info** screen displays an active connection, you have successfully completed the procedure.

## 4.6.2 Using TLS in Vista

Take the following steps to set up WPA, WPA2 or 802.1x security using TLS in Windows Vista.

1 Either select the AP to which you want to connect in the **Site Survey** screen (see Section 4.3 on page 49), or configure a profile (see Section 4.4 on page 56) in the normal way.

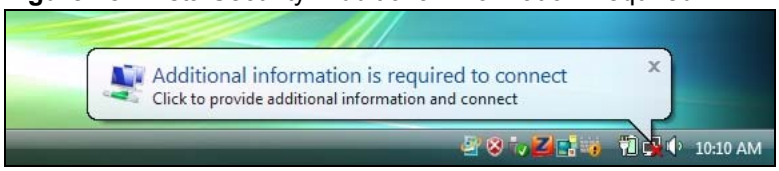
2 In the **WPA**, **WPA2** or **802.1x** security screen, select **TLS** as the **EAP Type**. Note that the **Login Name**, **Certificate** and **Validate Server Certificate** fields are not available (greyed-out).

3 Click **Next**.

4 In the **Summary** screen, click **Save**.

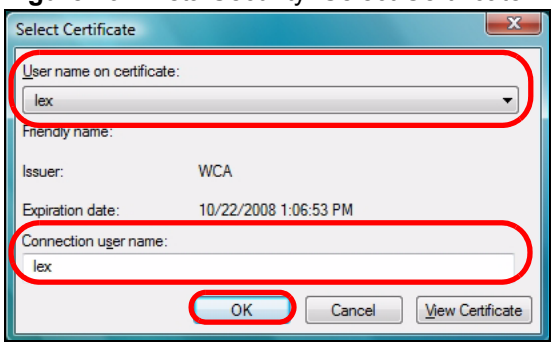
A message similar to the following appears in the bottom-right of your screen. Click the message.

**Figure 48** Vista Security: Additional Information Required




5 The **Select Certificate** screen displays. Select the certificate you want to use, and enter your username.

**Figure 49** Vista Security: Select Certificate




If you do not have the right certificate, or are not sure which certificate you should use, contact your network administrator.

6 Click **OK**. The **Select Certificate** screen disappears and the NWD310N tries to connect to the network. The ZyXEL utility's **Link Info** screen displays, showing the connection status (see Section 4.2 on page 47). If the **Link Info** screen displays an active connection, you have successfully completed the procedure.

# 5

# Maintenance

This chapter describes how to uninstall or upgrade the ZyXEL utility.

## 5.1 The About Screen

The **About** screen displays driver and utility version numbers of the NWD310N. To display the screen as shown below, click the about ( ) button.

**Figure 50** About

The following table describes the read-only fields in this screen.

**Table 20** About

| LABEL | DESCRIPTION |
|---|---|
| Driver Version | This field displays the version number of the NWD310N driver. |
| Utility Version | This field displays the version number of the ZyXEL utility. |

## 5.2 Uninstalling the ZyXEL Utility

Follow the steps below to remove (or uninstall) the ZyXEL utility from your computer.

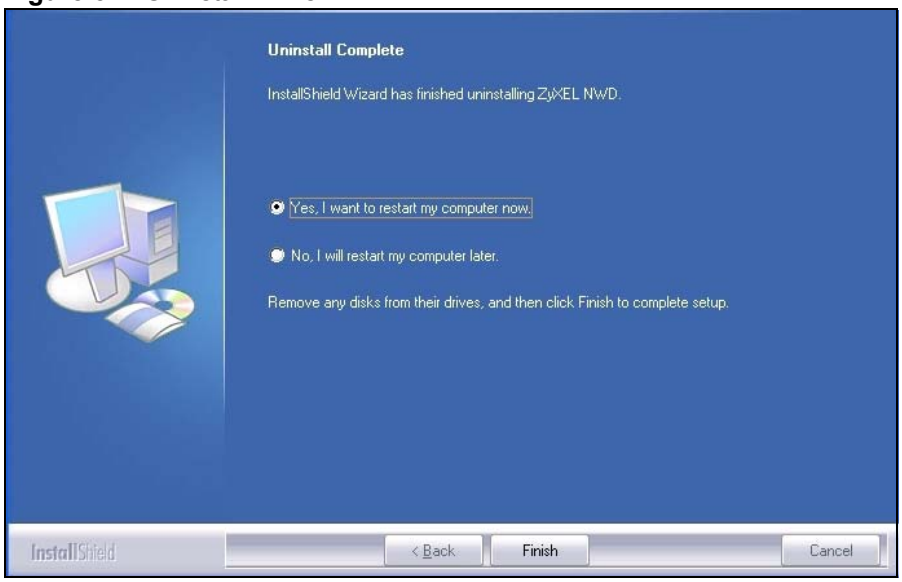
Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

1 Click **Start**, **(All) Programs**, **ZyXEL Wireless N PCI Utility**, **Uninstall ZyXEL Wireless N PCI Adapter Utility**.
2 When prompted, click **OK** or **Yes** to remove the driver and the utility software.

**Figure 51** Uninstall: Confirm

3 Click **Finish** to complete uninstalling the software and restart the computer when prompted.

**Figure 52** Uninstall: Finish


Uninstall Complete
InstallShield Wizard has finished uninstalling ZyXEL NWD.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
InstallShield
< Back
Finish
Cancel

## 5.3 Upgrading the ZyXEL Utility

Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

To perform the upgrade, follow the steps below.

1 Download the latest version of the utility from the ZyXEL web site and save the file on your computer.

2. Follow the steps in Section 5.2 on page 67 to remove the current ZyXEL utility from your computer.
3. Restart your computer when prompted.
4. Disconnect the NWD310N from your computer.
5. Double-click on the setup program for the new utility to start the ZyXEL utility installation.
6. Insert the NWD310N and check the version numbers in the **About** screen to make sure the new utility is installed properly.

# PART II
# Troubleshooting and Specifications

Troubleshooting (73)
Product Specifications (77)

# 6

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Accessing the Utility
- Link Quality
- Problems Communicating with Other Computers

## 6.1 Power, Hardware Connections, and LEDs

### The NWD310N does not turn on. None of the LEDs turn on.

1. Make sure the NWD310N is correctly installed (refer to your Quick Start Guide).
2. Restart the computer to which the NWD310N is attached.
3. If the problem continues, contact the vendor.

### One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.1 on page 21.
2. Check the hardware connections. See the Quick Start Guide and Section 1.1 on page 21.
3. Restart the computer to which the NWD310N is attached.
4. If the problem continues, contact the vendor.

## 6.2 Accessing the Utility

### I cannot access the Utility

1. Make sure the NWD310N is properly inserted and the LEDs are on. Refer to the Quick Start Guide for the LED descriptions.
2. Use the **Device Manager** to check for possible hardware conflicts. Click **Start**, **Settings**, **Control Panel**, **System**, **Hardware** and **Device Manager**. Verify the status of the NWD310N under **Network Adapter** (steps may vary depending on the version of Windows).
3. Install the NWD310N in another computer.
4. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

## 6.3 Link Quality

The link quality and/or signal strength is poor.

1. Scan for and connect to another AP with a better link quality using the **Site Survey** screen.
2. Move your computer closer to the AP or the peer computer(s) within the transmission range.
3. There may be too much radio interference (for example from a microwave oven, or another AP using the same channel) around your wireless network. Lower the output power of each AP.
4. Make sure there are not too many wireless stations connected to a wireless network.

## 6.4 Problems Communicating with Other Computers

The computer with the NWD310N installed cannot communicate with the other computer(s).

In Infrastructure Mode

- Make sure that the AP and the associated computers are turned on and working properly.
- Make sure the NWD310N computer and the associated AP use the same SSID.
- Change the AP and the associated wireless clients to use another radio channel if interference is high.
- Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Setting** screen.
- If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa.

In Ad-Hoc (IBSS) Mode

- Verify that the peer computer(s) is turned on.
- Make sure the NWD310N computer and the peer computer(s) are using the same SSID and channel.
- Make sure that the computer and the peer computer(s) share the same security settings.
- Change the wireless clients to use another radio channel if interference is high.

# 7

# Product Specifications

**Table 21** Product Specifications

| | |
|---|---|
| **PHYSICAL AND ENVIRONMENTAL** | |
| Product Name | NWD310N Draft 2.0 802.11n Wireless PCI Adapter |
| Interface | PCI bus 2.3 |
| Standards | IEEE 802.11b<br>IEEE 802.11g<br>IEEE 802.11n (Draft 2.0) |
| Operating Temperature | 0 ~ 55 degrees Celsius |
| Storage Temperature | -10 ~ 65 degrees Celsius |
| Operating Humidity | 20 ~ 95 % (non-condensing) |
| Storage Humidity | 20 ~ 95 % (non-condensing) |
| Power Consumption | TX: < 750 mA<br>RX: < 650mA |
| Voltage | 3.3 V |
| Weight | 40 g |
| Dimensions | 122 x 121 x 221 mm |
| **RADIO SPECIFICATIONS** | |
| Media Access Protocol | IEEE 802.11 |
| Frequency | Industrial Scientific Medical Band<br>2.4 ~ 2.4835 GHz |
| Operating Channels | North American and Taiwan: 11<br>Europe: 13 |
| Data Rate | IEEE 802.11b: 11Mbps with automatic fallback to 5.5, 2, 1 Mbps<br>IEEE 802.11g: 54Mbps with automatic fallback to 48, 36, 24, 18, 12, 9, 6 Mbps<br>IEEE 802.11n (draft): up to 300 Mbps |
| Modulation | IEEE 802.11b: CCK (11 and 5.5 Mbps), DQPSK (2 Mbps) and DBPSK (1 Mbps)<br>IEEE 802.11g: OFDM with BPSK, QPSK and 16/64-QAM sub-Carrier modulations<br>IEEE 802.11n (draft): |
| Average Output Power | Tolerance: +/- 1.5dBm<br>IEEE 802.11b: 18 dBm at 11 Mbps<br>IEEE 802.11g: 15 dBm at 54 Mbps<br>IEEE 802.11n (draft): 15 dBm at HT20, 13 dBm at HT40 |

**Table 21** Product Specifications (continued)

| | |
|---|---|
| Receiver Sensitivity | Tolerance: +/- 1 dBm<br>IEEE 802.11b: -84 dBm at 11 Mbps<br>IEEE 802.11g: -72 dBm at 54 Mbps<br>IEEE 802.11n (draft): -70 dBm at HT20, -67 dBm at HT40 |
| **SOFTWARE SPECIFICATIONS** | |
| Device Drivers | Windows Vista<br>Windows XP 64-bit<br>Windows XP<br>Windows 2000<br>MAC OS 10.3 & 10.4 |
| Security | 64/128/152-bit WEP<br>WPA/WPA-PSK/WPA2/WPA2-PSK<br>IEEE 802.1x<br>WPS (WiFi Protected Setup) Certified |
| Roaming | IEEE 802.11b/g/n compliant |

# PART III Appendices and Index

The appendices provide general information. Some details may not apply to your NWD310N.


Setting up Your Computer's IP Address (81)

Wireless LANs (103)

Windows Wireless Management (117)

Legal Information (139)

Customer Support (143)

Index (149)

# A

# Setting up Your Computer's IP Address

The purpose of this appendix is to show you how to configure an IP address on your computer depending on what operating system you have. It does NOT mean that your NWD310N supports all these operating systems. To see what operating systems your NWD310N supports, refer to Chapter 7 on page 77.

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

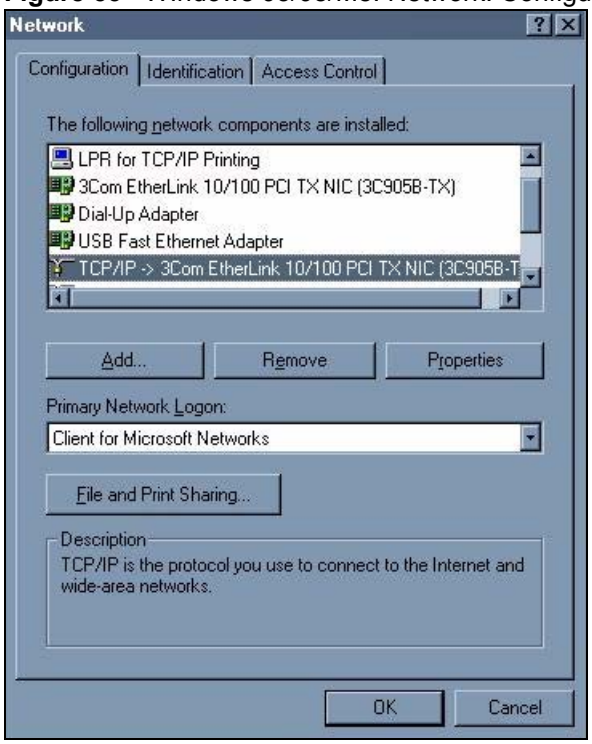
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the NWD310N's LAN port.

## Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 53** WIndows 95/98/Me: Network: Configuration




## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

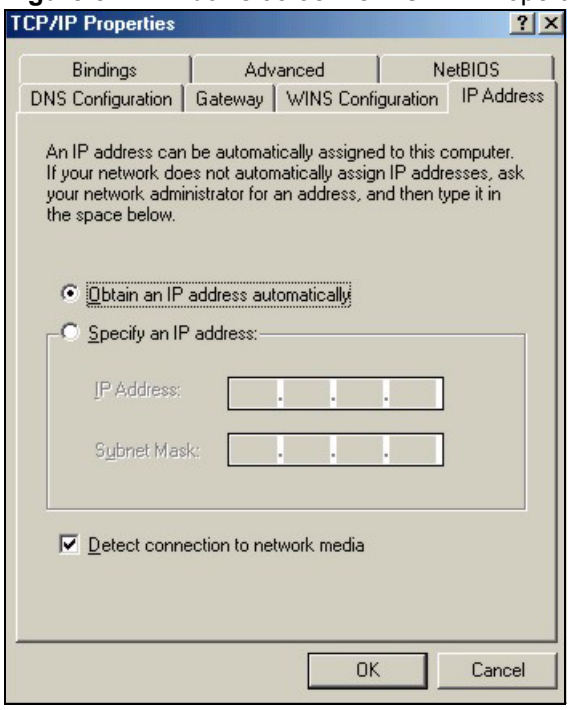
If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

## Configuring

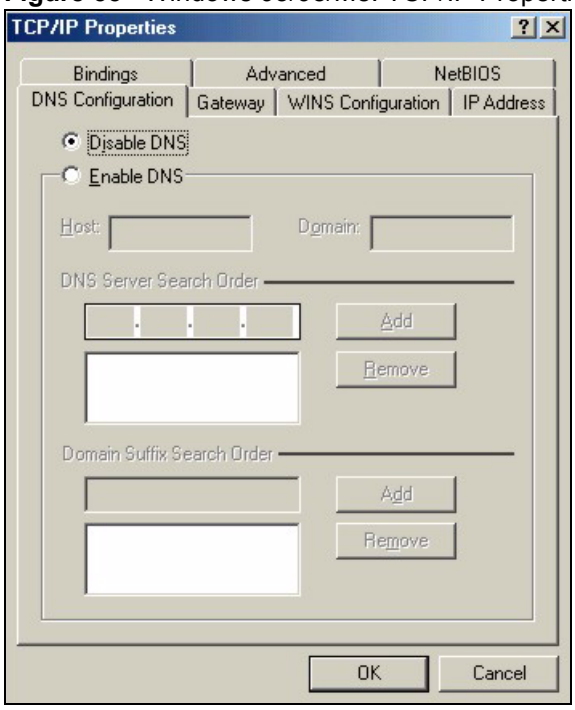
1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
2. Click the **IP Address** tab.
   - If your IP address is dynamic, select **Obtain an IP address automatically**.
   - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 54** Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3. Click the **DNS** Configuration tab.
   - If you do not know your DNS information, select **Disable DNS**.
   - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 55** Windows 95/98/Me: TCP/IP Properties: DNS Configuration




4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your NWD310N and restart your computer when prompted.

### Verifying Settings

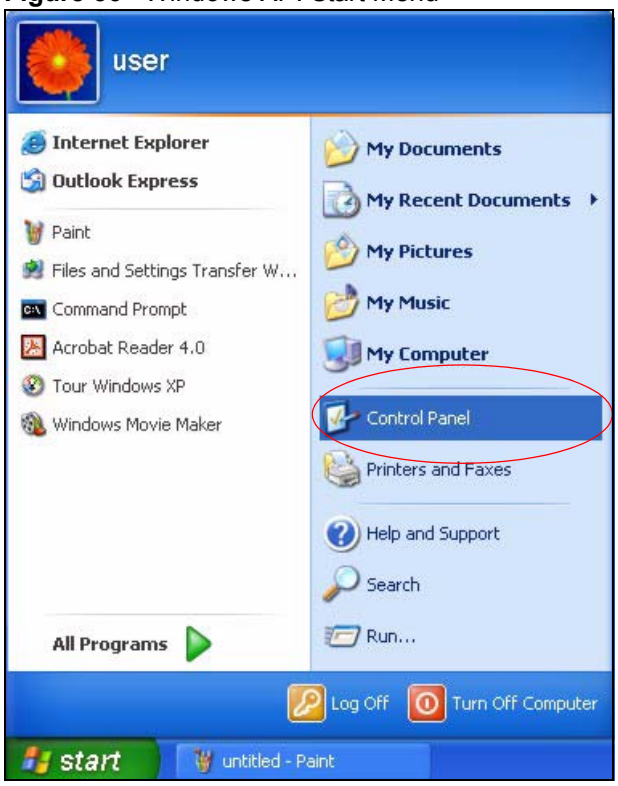
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 56** Windows XP: Start Menu

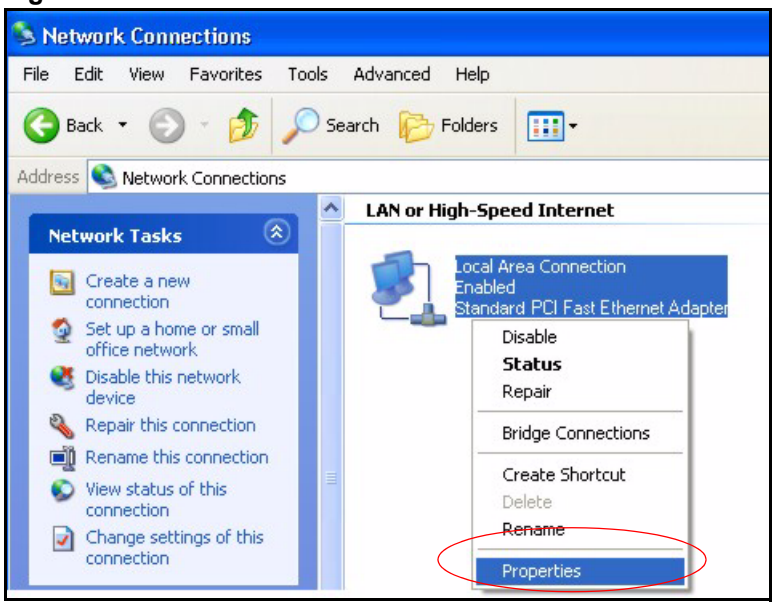



2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 57** Windows XP: Control Panel

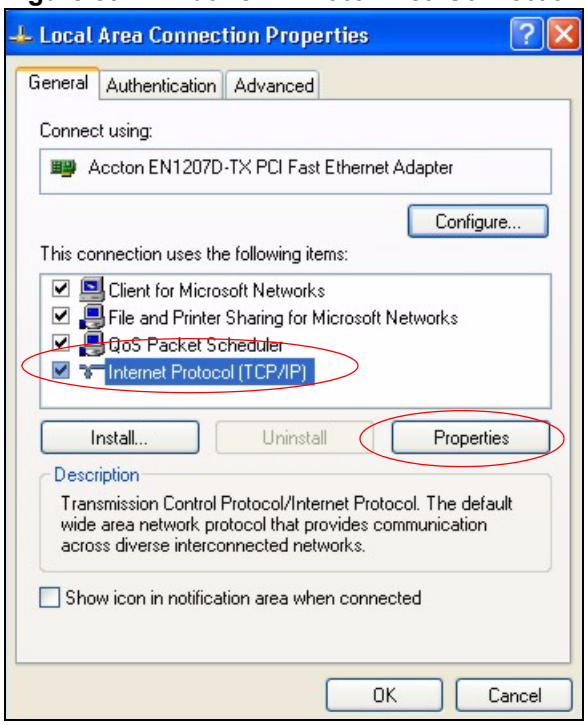
3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 58** Windows XP: Control Panel: Network Connections: Properties




**4** Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

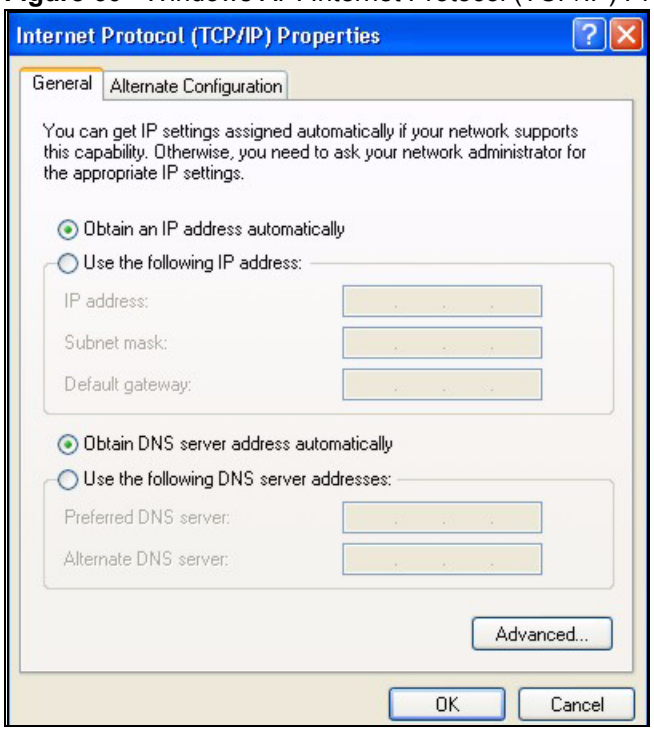
**Figure 59** Windows XP: Local Area Connection Properties


Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

**5** The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

**Figure 60** Windows XP: Internet Protocol (TCP/IP) Properties

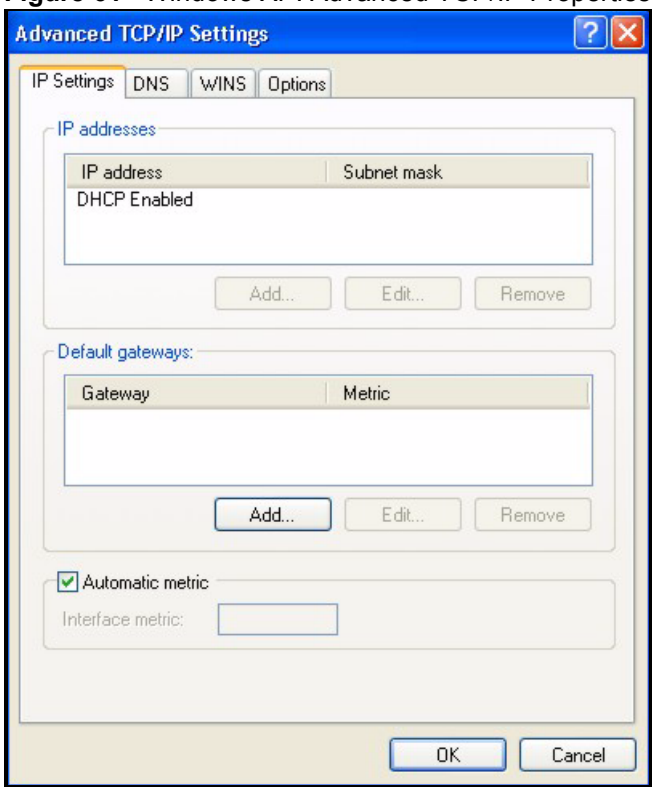

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

**Figure 61** Windows XP: Advanced TCP/IP Properties

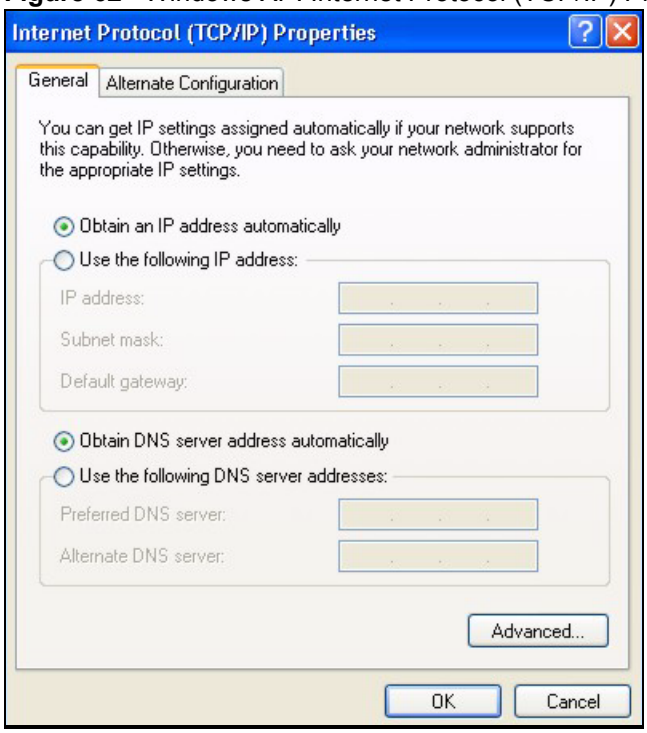



7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 62** Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your NWD310N and restart your computer (if prompted).

### Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

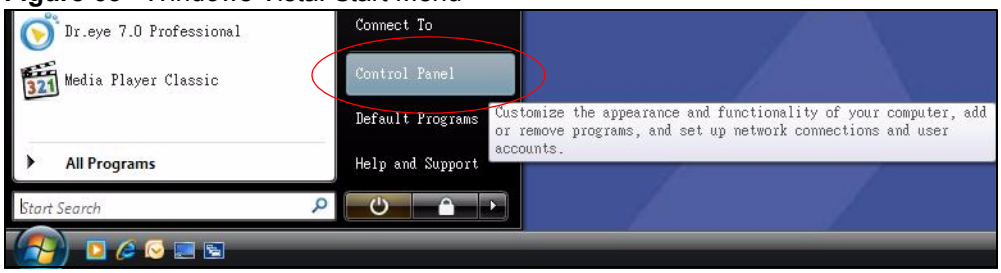
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

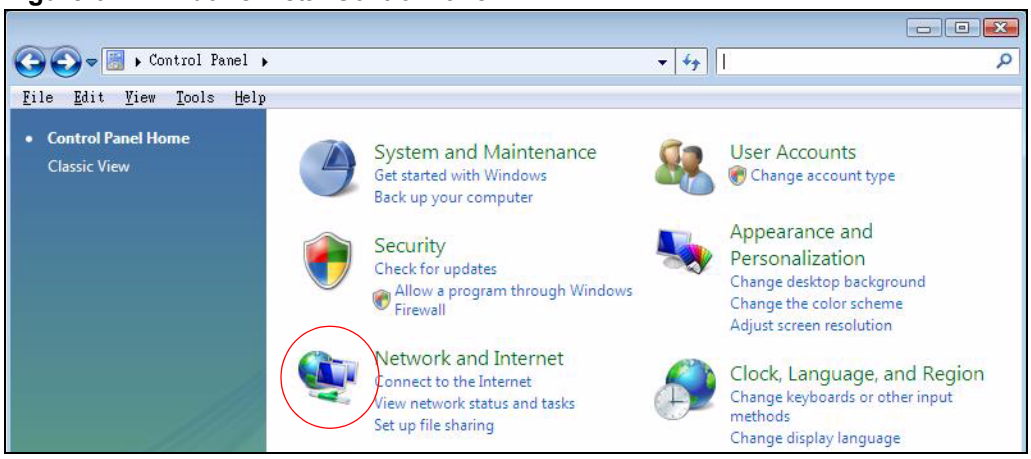
1 Click the **Start** icon, **Control Panel**.

**Figure 63** Windows Vista: Start Menu


Dr.eye 7.0 Professional
Media Player Classic
All Programs
Start Search
Connect To
Control Panel
Default Programs
Help and Support
Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

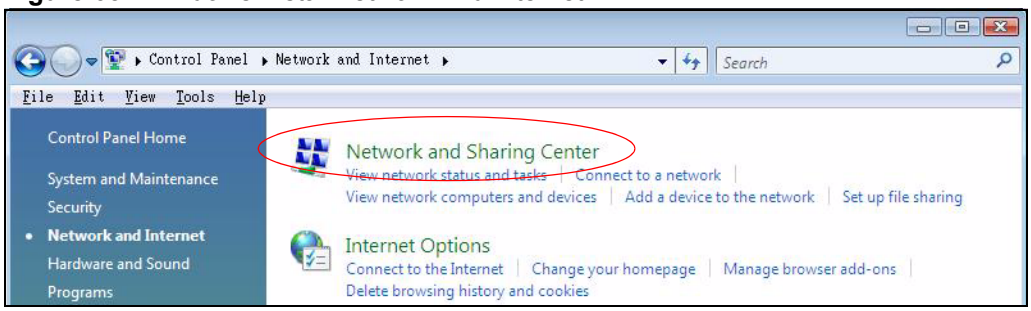
**2** In the **Control Panel**, double-click **Network and Internet**.

**Figure 64** Windows Vista: Control Panel



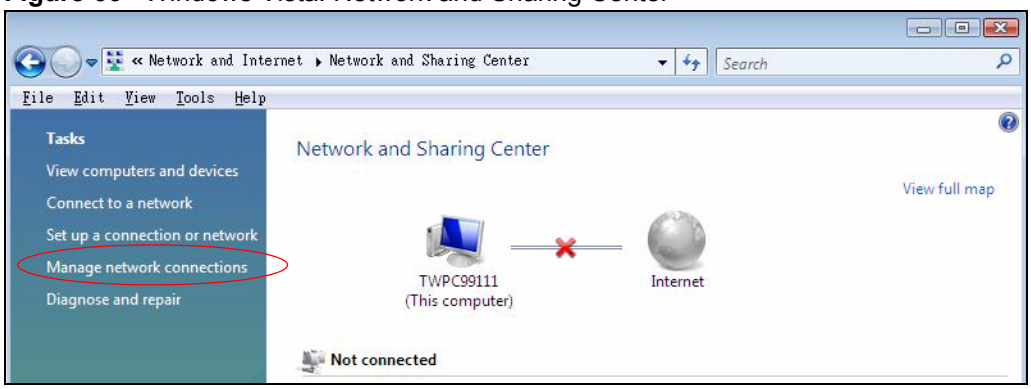

**3** Click **Network and Sharing Center**.

**Figure 65** Windows Vista: Network And Internet




**4** Click **Manage network connections**.

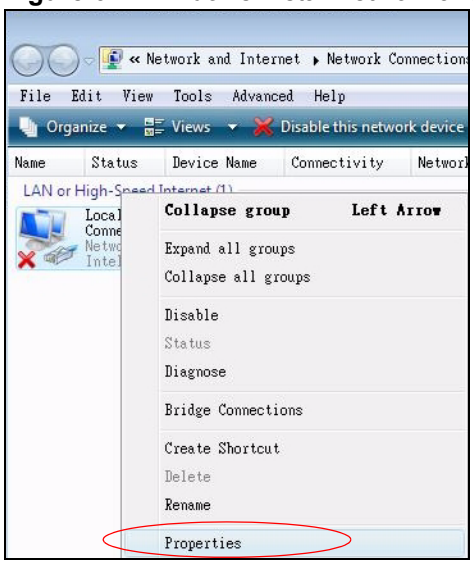
**Figure 66** Windows Vista: Network and Sharing Center



**5** Right-click **Local Area Connection** and then click **Properties**.

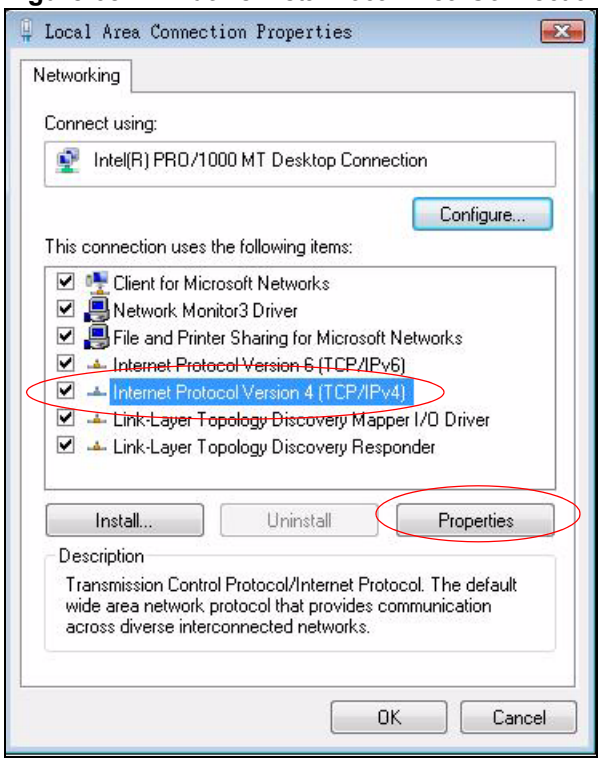
During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

**Figure 67** Windows Vista: Network and Sharing Center



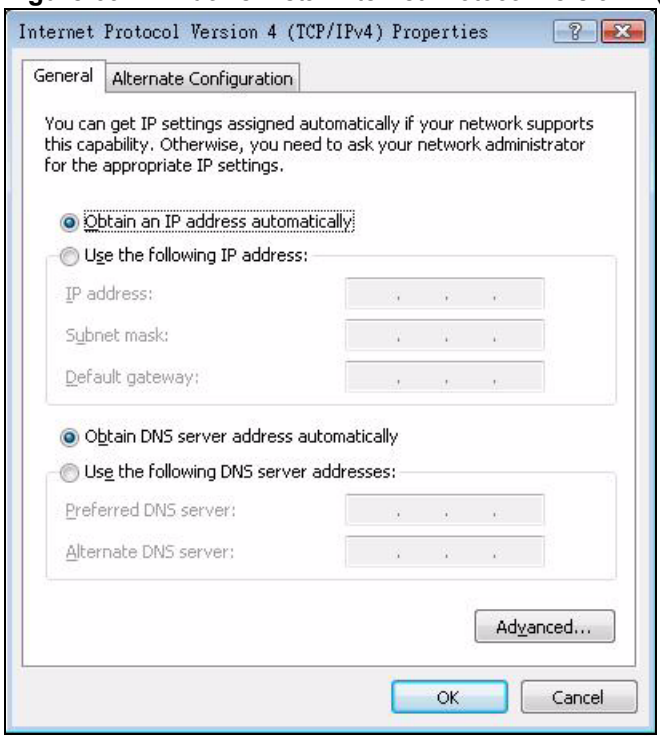

**6** Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

**Figure 68** Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).
- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

**Figure 69** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties

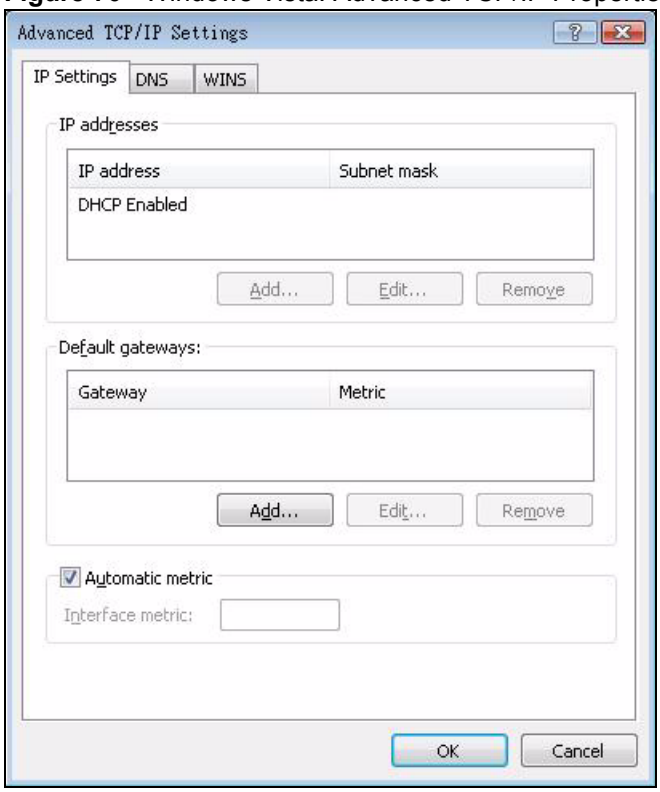

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

**Figure 70** Windows Vista: Advanced TCP/IP Properties

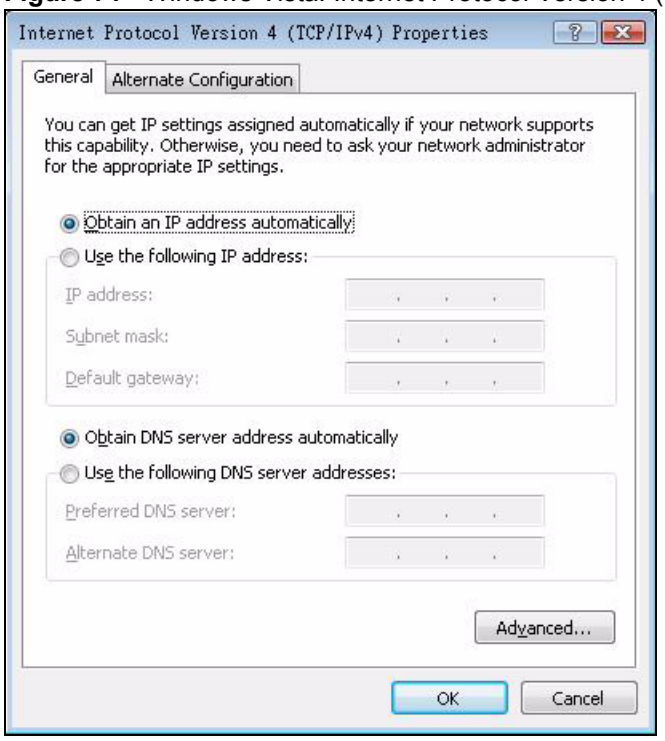



**9** In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 71** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

**10** Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

**11** Click **Close** to close the **Local Area Connection Properties** window.

**12** Close the **Network Connections** window.

**13** Turn on your NWD310N and restart your computer (if prompted).

### Verifying Settings

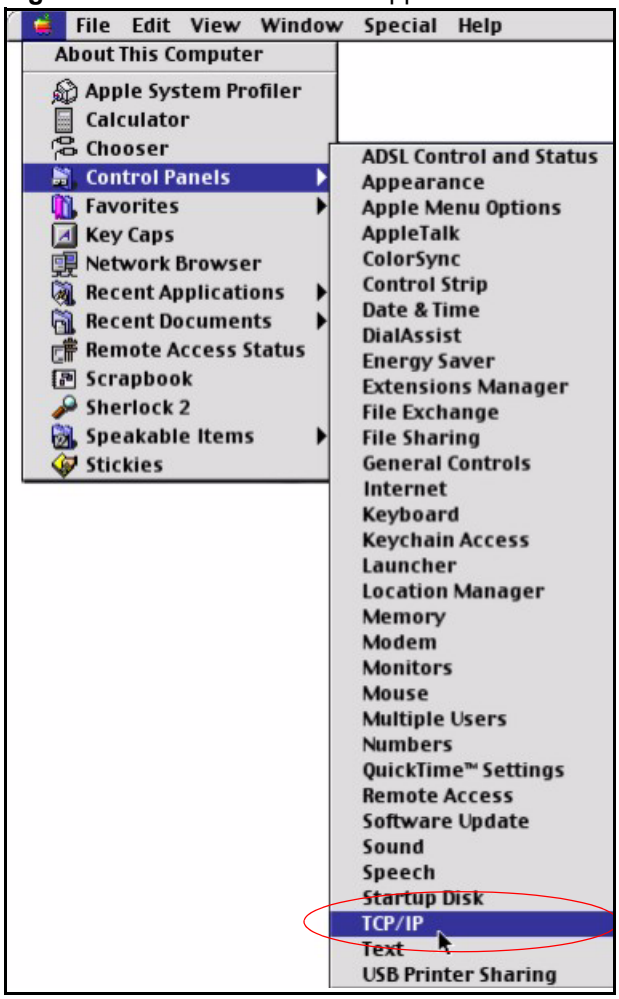
**1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

**2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

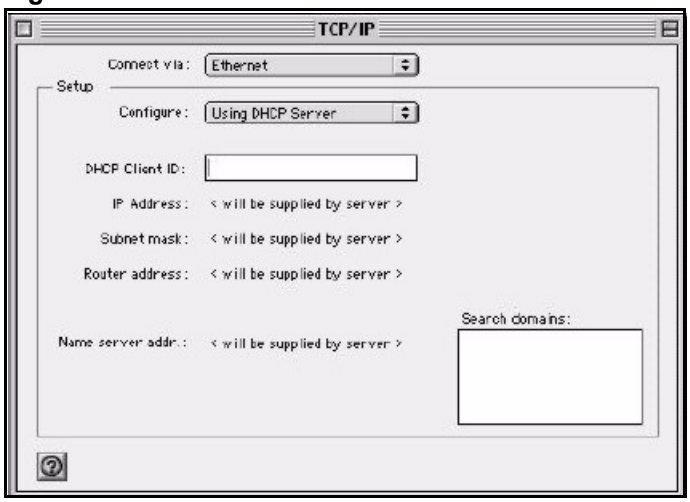
**1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 72** Macintosh OS 8/9: Apple Menu




**2** Select **Ethernet built-in** from the **Connect via** list.

**Figure 73** Macintosh OS 8/9: TCP/IP




**3** For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your NWD310N in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your NWD310N and restart your computer (if prompted).

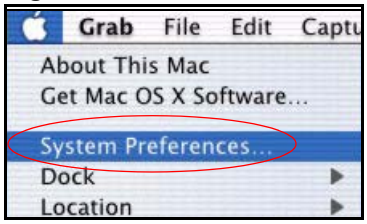
### Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

## Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 74** Macintosh OS X: Apple Menu

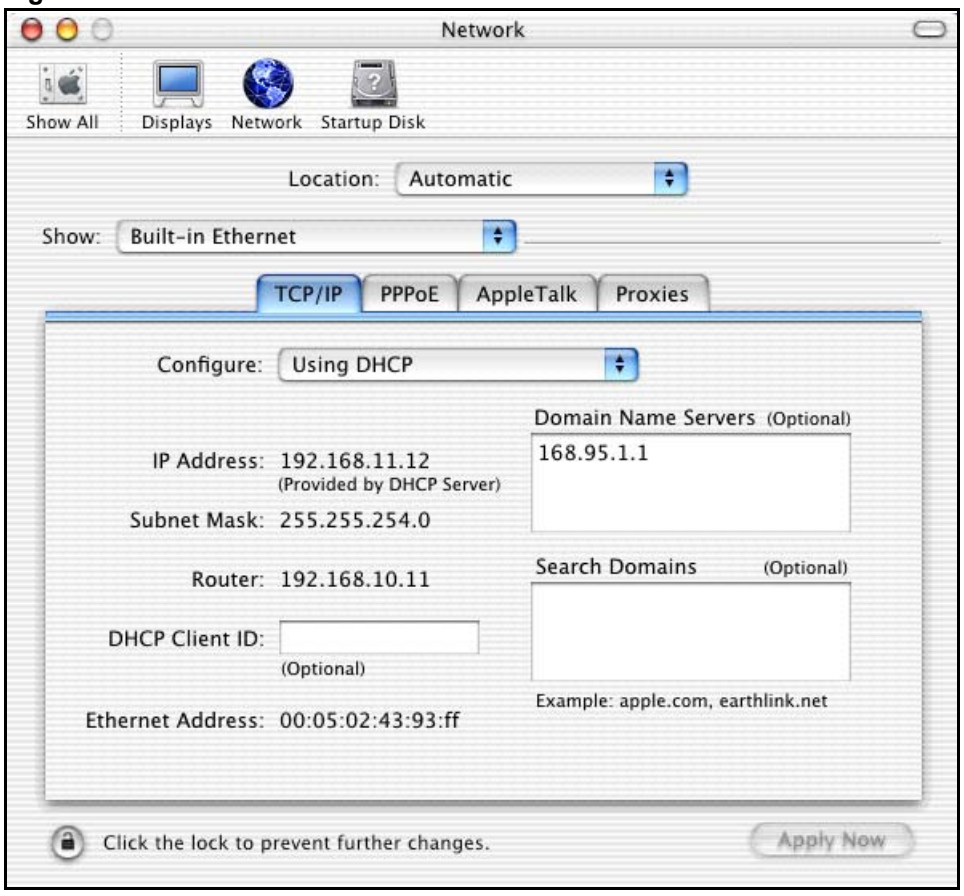



2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 75** Macintosh OS X: Network




4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your NWD310N in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your NWD310N and restart your computer (if prompted).

### Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

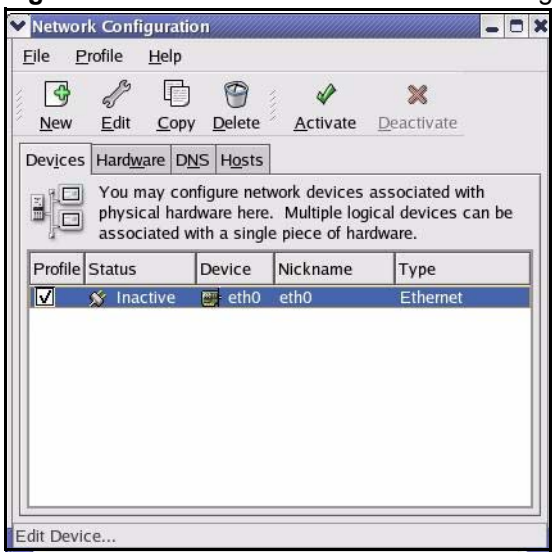
Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 76** Red Hat 9.0: KDE: Network Configuration: Devices




2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

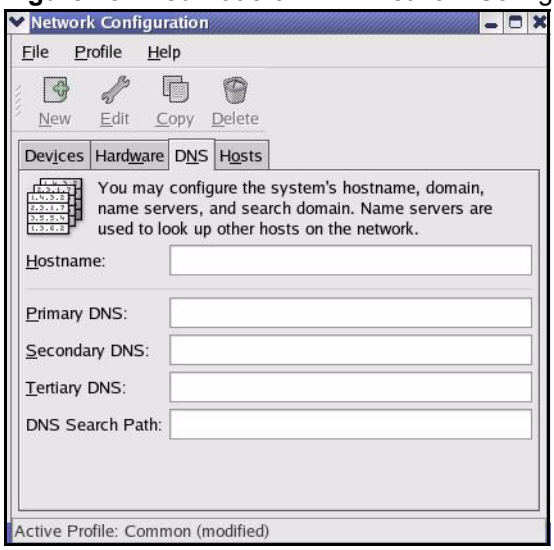
**Figure 77** Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 78** Red Hat 9.0: KDE: Network Configuration: DNS




5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

**Figure 79** Red Hat 9.0: KDE: Network Configuration: Activate

Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 80** Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 81** Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 82** Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 83** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 84** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

# B

# Wireless LANs

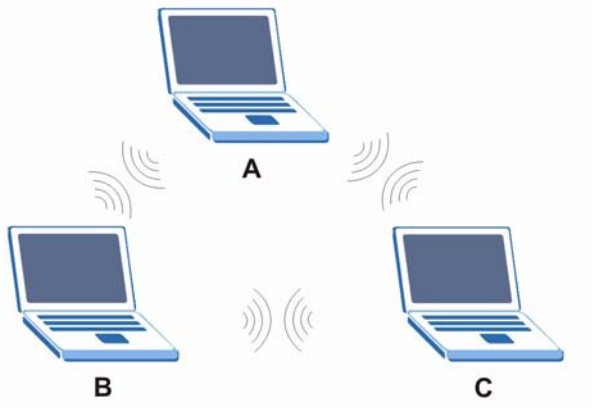
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

**Figure 85** Peer-to-Peer Communication in an Ad-hoc Network

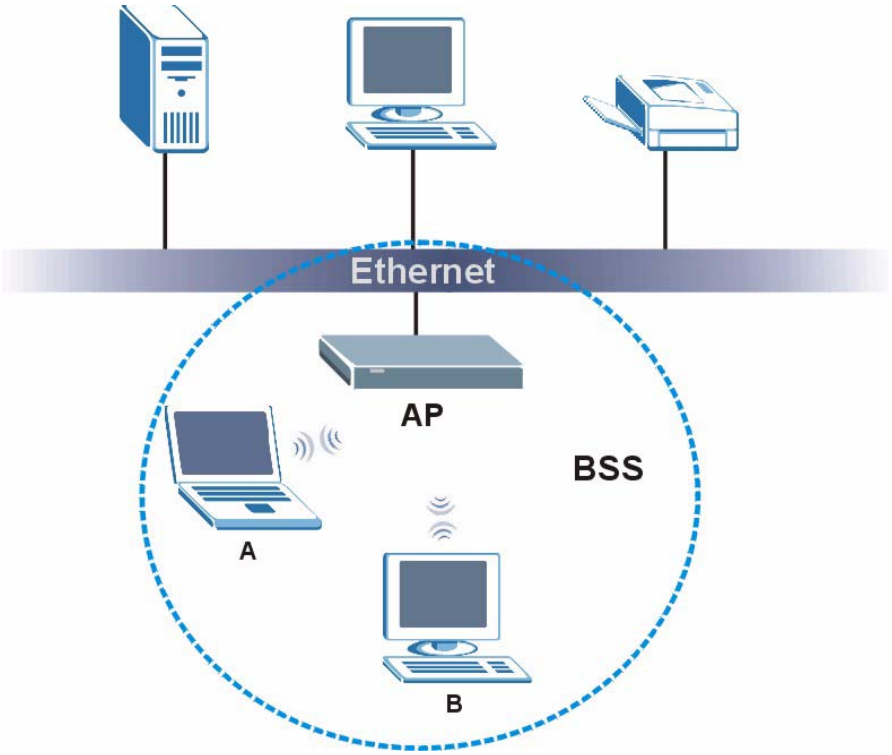



### BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

**Figure 86** Basic Service Set



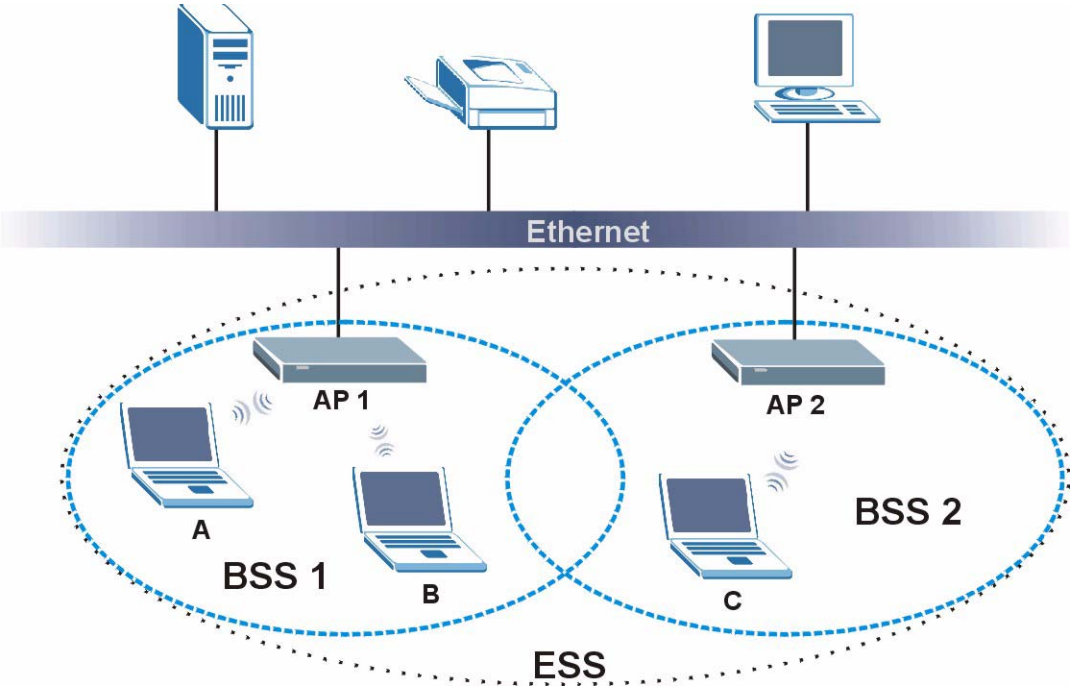

## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

**Figure 87** Infrastructure WLAN




## Channel

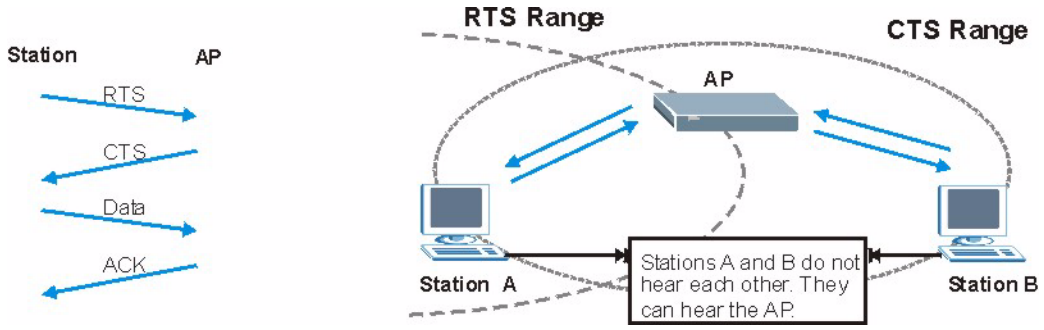
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 88** RTS/CTS




When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NWD310N uses long preamble.

The wireless devices MUST use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 22** IEEE 802.11g

| DATA RATE (MBPS) | MODULATION |
|---|---|
| 1 | DBPSK (Differential Binary Phase Shift Keyed) |
| 2 | DQPSK (Differential Quadrature Phase Shift Keying) |
| 5.5 / 11 | CCK (Complementary Code Keying) |
| 6/9/12/18/24/36/48/54 | OFDM (Orthogonal Frequency Division Multiplexing) |

## Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the NWD310N are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NWD310N identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NWD310N.

**Table 23** Wireless Security Levels

| SECURITY LEVEL | SECURITY TYPE |
|---|---|
| Least Secure | Unique SSID (Default) |
| | Unique SSID with Hide SSID Enabled |
| | MAC Address Filtering |
| | WEP Encryption |
| | IEEE802.1x EAP with RADIUS Server Authentication |
| | Wi-Fi Protected Access (WPA) |
| Most Secure | WPA2 |

You must enable the same wireless security settings on the NWD310N and on all wireless clients that you want to associate with it.

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
  Determines the identity of the users.
- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

### Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

### EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

### PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

### LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

# Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 24** Comparison of EAP Authentication Types

| | EAP-MD5 | EAP-TLS | EAP-TTLS | PEAP | LEAP |
|---|---|---|---|---|---|
| Mutual Authentication | No | Yes | Yes | Yes | Yes |
| Certificate – Client | No | Yes | Optional | Optional | No |
| Certificate – Server | No | Yes | Yes | Yes | No |
| Dynamic Key Exchange | No | Yes | Yes | Yes | Yes |
| Credential Integrity | None | Strong | Strong | Strong | Moderate |
| Deployment Difficulty | Easy | Hard | Moderate | Moderate | Moderate |
| Client Identity Protection | No | No | Yes | Yes | No |

# WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

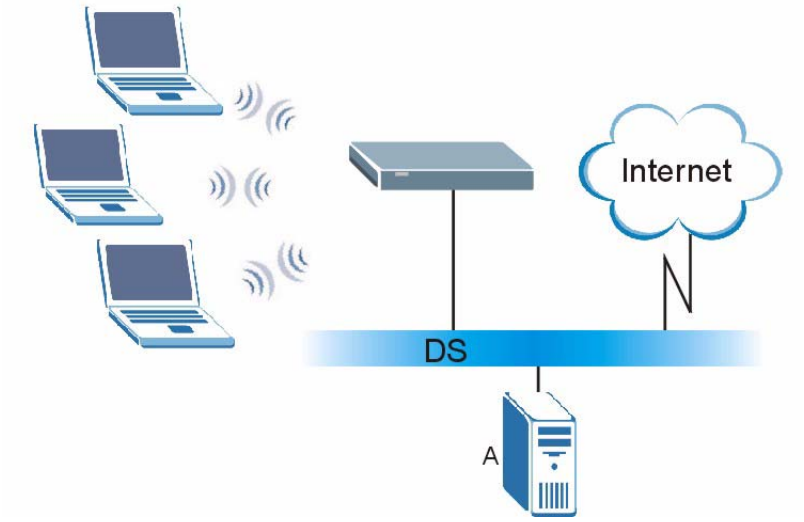
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

## WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 89** WPA(2) with RADIUS Application Example




## WPA(2)-PSK Application Example

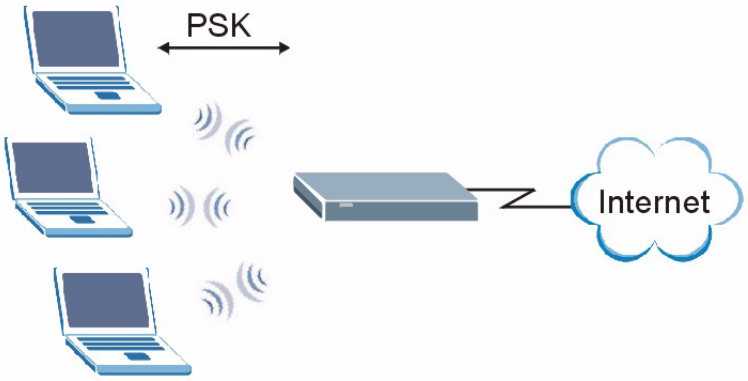
A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

**Figure 90** WPA(2)-PSK Authentication




# Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 25** Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|---|---|---|---|
| Open | None | No | Disable |
| | | | Enable without Dynamic WEP Key |
| Open | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| Shared | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| WPA | TKIP/AES | No | Enable |
| WPA-PSK | TKIP/AES | Yes | Disable |
| WPA2 | TKIP/AES | No | Enable |
| WPA2-PSK | TKIP/AES | Yes | Disable |

# Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

# Antenna Characteristics

## Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

## Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

## Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

# Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

# Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

C

# Windows Wireless Management

This appendix shows you how to manage your NWD310N using the Windows Vista and Windows XP wireless configuration tools.

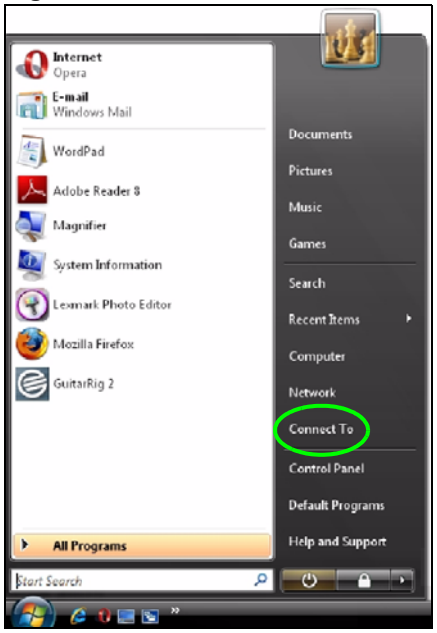
## Windows Vista

Take the following steps to connect to a wireless network using the Windows Vista wireless configuration tool (WLAN AutoConfig).

### Connecting to a Wireless Network

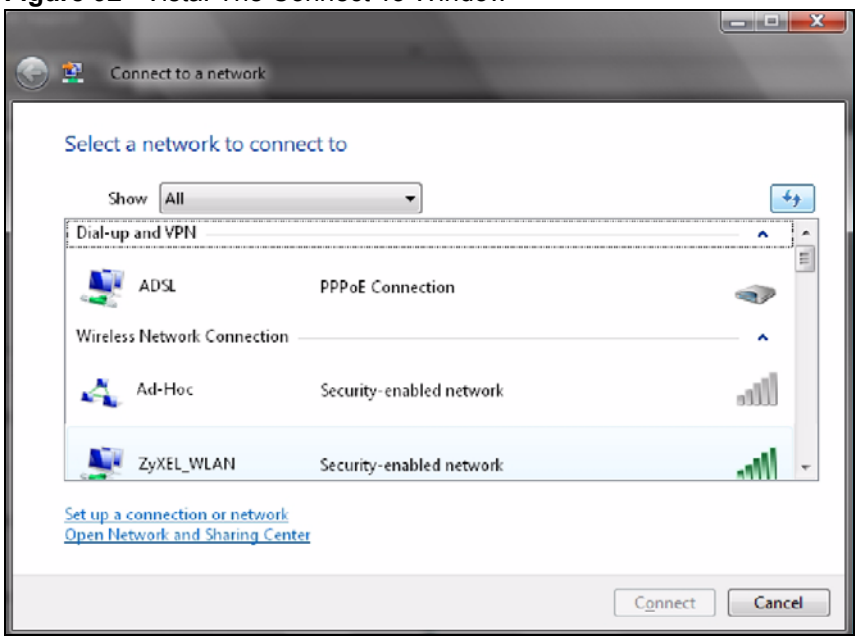
1 In the Windows Vista taskbar, click **Start** ( ) > **Connect To**.

**Figure 91** Vista: Start Menu



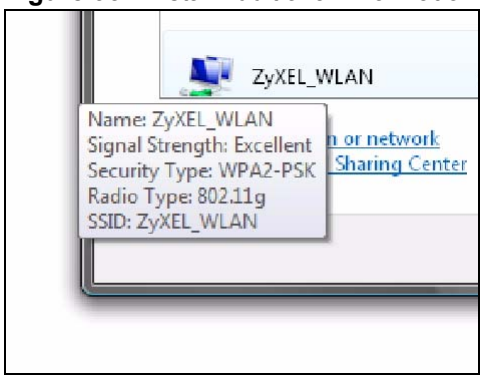

The **Connect To** window displays, showing all available networks.

**Figure 92** Vista: The Connect To Window




The security status of each wireless network displays, as well as an indication of its signal strength. If you use the mouse pointer to hover over a network's entry, additional information about the network displays.

**Figure 93** Vista: Additional Information

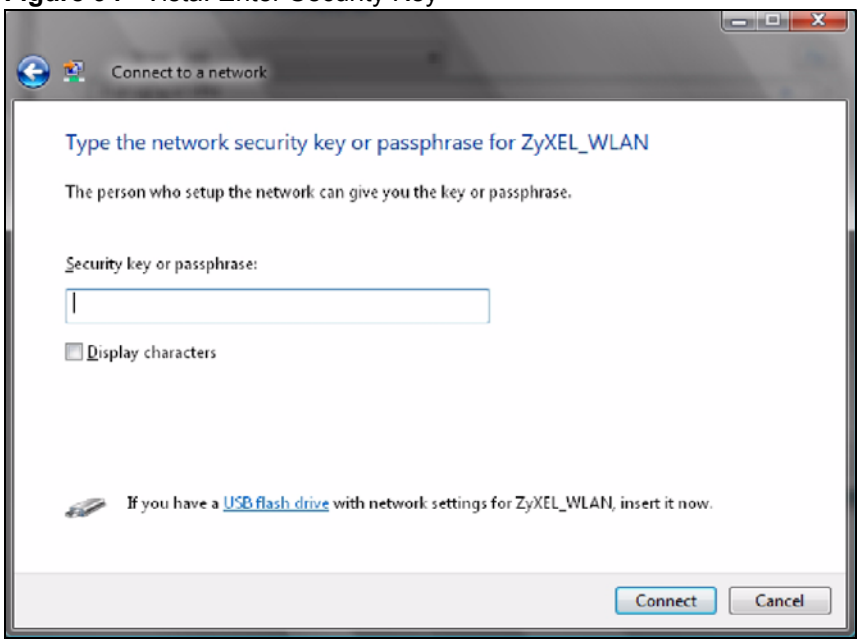



2 Double-click the network's name to join the network, or select a network and click **Connect**.

If the network to which you want to connect does not display, see the section on setting up a connection manually on page 120.

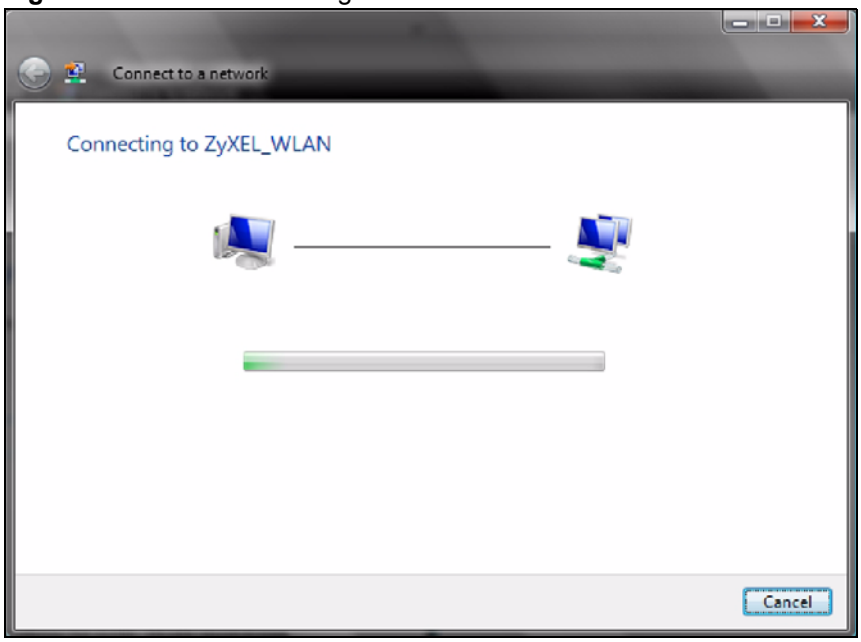
3 If security is enabled, you may be prompted to enter your security key.

**Figure 94** Vista: Enter Security Key


Connect to a network
Type the network security key or passphrase for ZyXEL_WLAN
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for ZyXEL_WLAN, insert it now.
Connect
Cancel

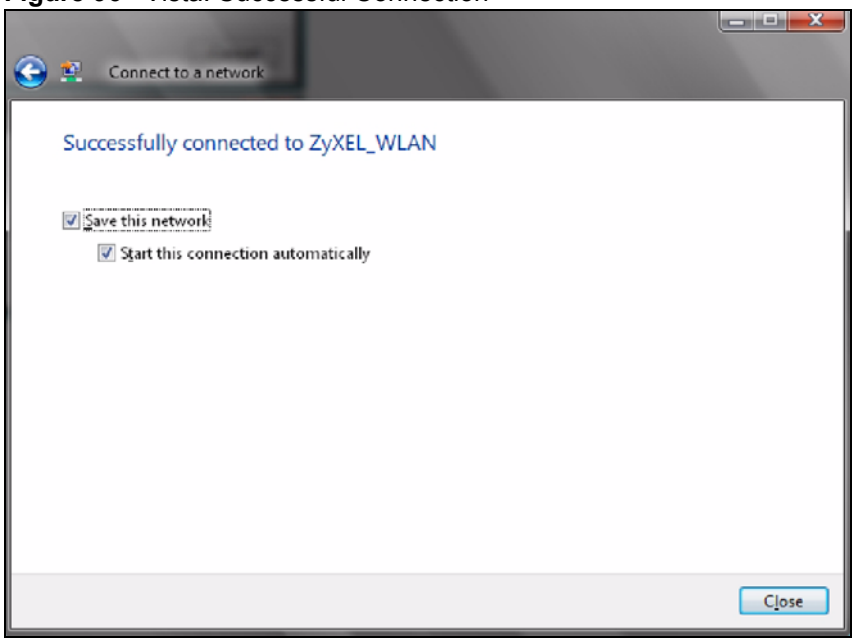
Your computer tries to connect to the wireless network.

**Figure 95** Vista: Connecting




If your computer has connected to the wireless network successfully, the following screen displays.

**Figure 96** Vista: Successful Connection




4 If you will use this network again, ensure that **Save this network** is selected. If you save the network, you do not have to configure its settings again.

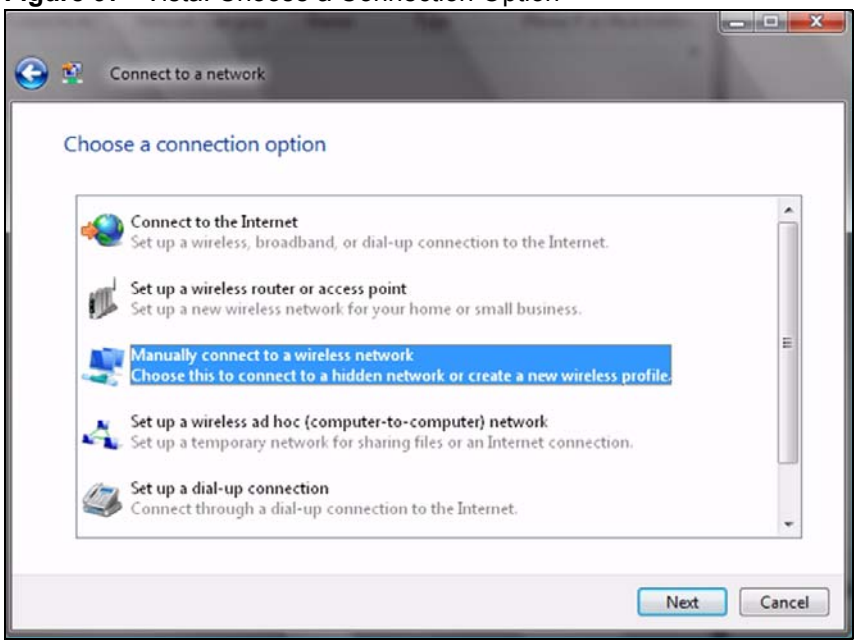
5 Select **Start this connection automatically** if you want Windows to always try to use this network when you start up your computer. If you do not select this (but select **Save this network**) you can connect manually each time by clicking **Start** > **Connect to** and selecting the network's name from the list.

## Connecting to a Network Manually

If the wireless network to which you want to connect does not appear in the **Connect to** window (if your network's SSID is hidden, for example), take the following steps to configure your network connection manually

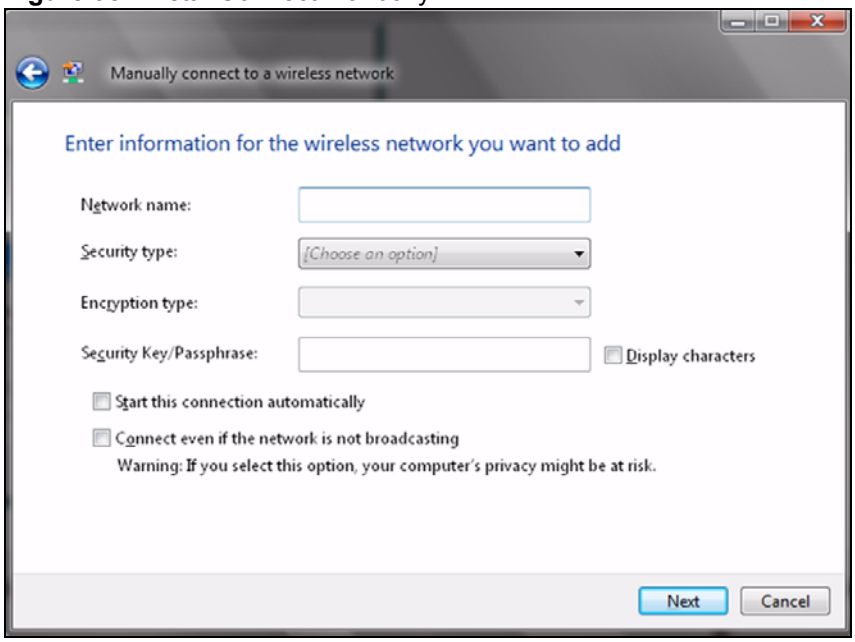
1 Click **Set up a connection or network** at the bottom of the **Connect to** screen. The following screen displays.

**Figure 97** Vista: Choose a Connection Option


Connect to a network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a wireless router or access point
Set up a new wireless network for your home or small business.
Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.
Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.
Set up a dial-up connection
Connect through a dial-up connection to the Internet.
Next
Cancel

**2** Click **Manually connect to a wireless network**. The following screen displays.

**Figure 98** Vista: Connect Manually


Manually connect to a wireless network
Enter information for the wireless network you want to add
Network name:
Security type:
(Choose an option)
Encryption type:
Security Key/Passphrase:
Display characters
Start this connection automatically
Connect even if the network is not broadcasting
Warning: If you select this option, your computer's privacy might be at risk.
Next
Cancel

The following table describes the labels in this screen.

**Table 26** Vista: Connect Manually

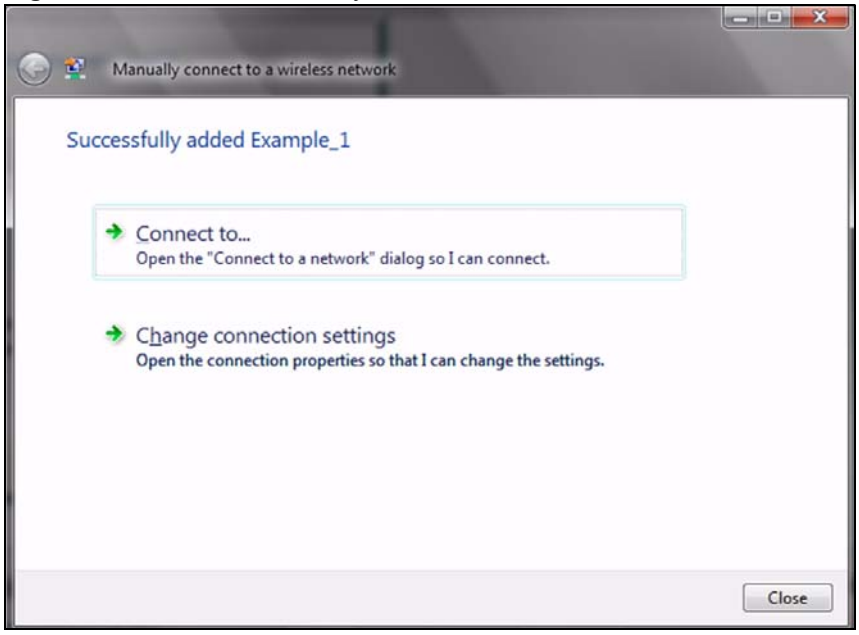
| LABEL | DESCRIPTION |
|---|---|
| Network name | Enter your network's SSID (Service Set IDentifier). |
| Security type | Select the type of security used by the network to which you want to connect. The types of available security shown depend on your computer's wireless client.<br>In this field, **WPA(2)-Personal** is the same as **WPA(2)-PSK**, and **WPA(2)-Enterprise** is the same as **WPA(2)** |

**Table 26** Vista: Connect Manually

| LABEL | DESCRIPTION |
|---|---|
| Encryption type | Select the type of encryption used by the network.<br>When you use **WEP** or **802.1x**, **WEP** displays.<br>When you use a **WPA** mode (**WPA(2)-Personal** or **WPA(2)-Enterprise**) you can choose **AES** or **TKIP** (if supported by your computer's wireless client). |
| Security Key / Passphrase | If your network uses **WEP** or **WPA(2)-Personal** security, enter the key here. |
| Display Characters | Select this if you do not want the security key characters to be hidden. |
| Start this connection automatically | Select this box if you always want to try to connect to this network at startup. If you leave this box unchecked, you will need to connect manually each time. |
| Connect even if the network is not broadcasting | Select this box if you always want to try to connect to this network at startup, even if the network is not broadcasting its SSID. The warning in this field refers to the fact that if you do this, your computer sends out probe request packets, which contain the network's SSID and could be used by an attacker to access the network. |
| Next | Click this to save your settings and move on to the next page. |
| Cancel | Click this to stop setting up your network. |

**3** When you have finished filling in the fields, click **Next**. the following screen displays.

**Figure 99** Vista: Successfully Added Network


Manually connect to a wireless network
Successfully added Example_1
Connect to...
Open the "Connect to a network" dialog so I can connect.
Change connection settings
Open the connection properties so that I can change the settings.
Close

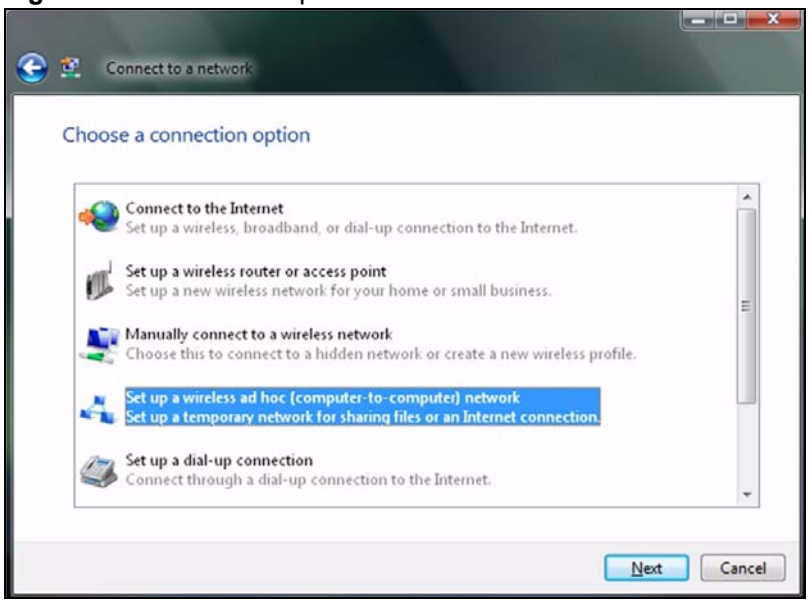
**4** If you want to make any changes to the settings you just configured, click **Change connection settings**. Otherwise, click **Connect to...**. In the window that displays, double-click the new network's name to connect to the network.

## Setting Up An Ad-Hoc Network

Take the following steps to set up a wireless connection between two computers in Windows Vista.

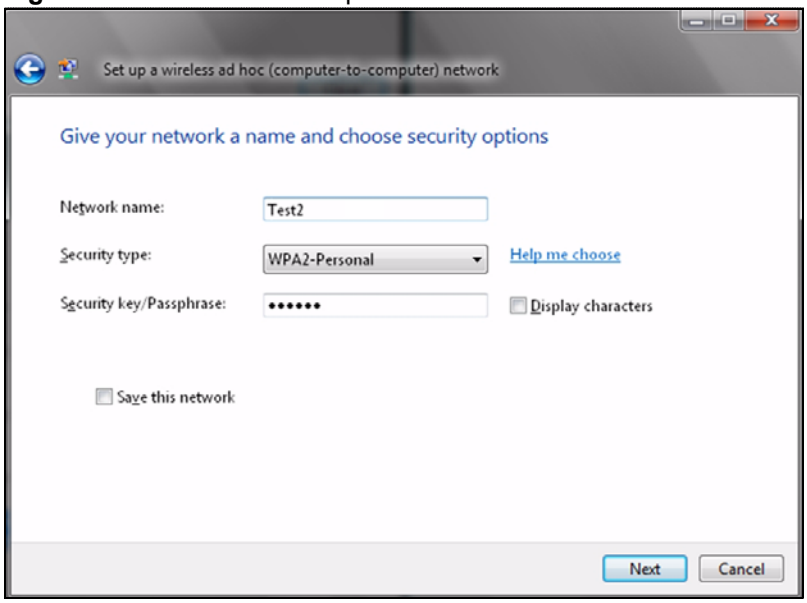
1 Click **Start** ( ) > **Connect To**. In the **Connect to** screen, click **Set up a connection or network**. The following screen displays.

**Figure 100** Vista: Set Up An Ad-hoc Network


Connect to a network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a wireless router or access point
Set up a new wireless network for your home or small business.
Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.
Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.
Set up a dial-up connection
Connect through a dial-up connection to the Internet.
Next
Cancel

2 Select **Set up a wireless ad hoc (computer-to-computer) network** and click **Next**. The following screen displays.

**Figure 101** Vista: Ad-hoc Options




3 Enter the **Network name** (SSID) you want to use for your network. Select a **Security type**. If you are not sure what kind of security you want to use, click the **Help me choose** link.

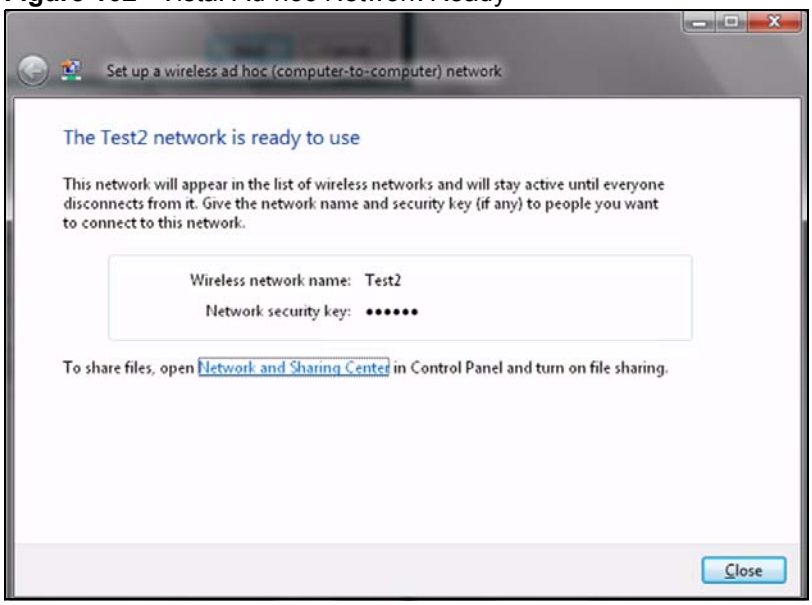
Make sure all the wireless clients on your ad-hoc network can support the type of security you select.

4 Enter the **Security key/Passphrase**. Everybody on the network must enter this key in their computer's wireless client in order to access the network. If you want to see the characters you entered, select the **Display characters** box. Otherwise, leave it empty (dots display instead of the characters).

5 If you will use this ad-hoc network again, select the **Save this network** box. If you do this, the next time you click **Start** > **Connect to**, you can select the network from the list.

6 Click **Next**. The following screen displays.

**Figure 102** Vista: Ad-hoc Network Ready


Set up a wireless ad hoc (computer-to-computer) network
The Test2 network is ready to use
This network will appear in the list of wireless networks and will stay active until everyone disconnects from it. Give the network name and security key (if any) to people you want to connect to this network.
Wireless network name: Test2
Network security key: ••••••
To share files, open Network and Sharing Center in Control Panel and turn on file sharing.
Close

7 If you want to share files with other computers on the ad-hoc network, or let other computers use your Internet connection, click the **Network and Sharing Center** link. Otherwise, click **Close**.

# Windows XP

Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon ( ) in most screens, move the cursor to the item that you want the information about and click to view the help.

## Activating Wireless Zero Configuration

1 Click **Start**, **Control Panel** and double-click **Network Connections**.

2 Double-click on the icon for wireless network connection.

3 The status window displays as shown below. Click **Properties**.

**Figure 103** Windows XP SP1: Wireless Network Connection Status

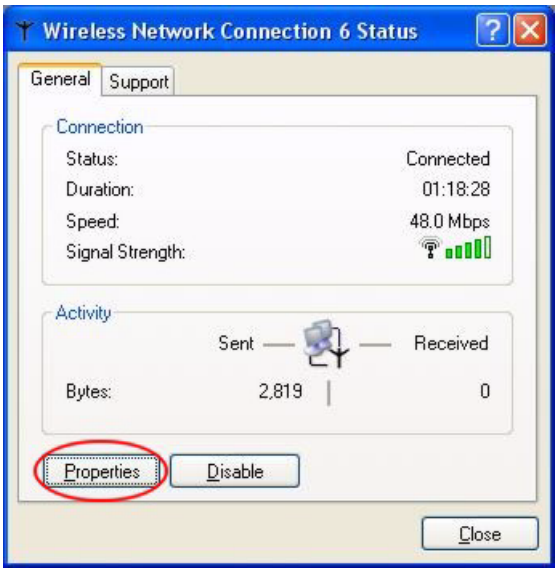
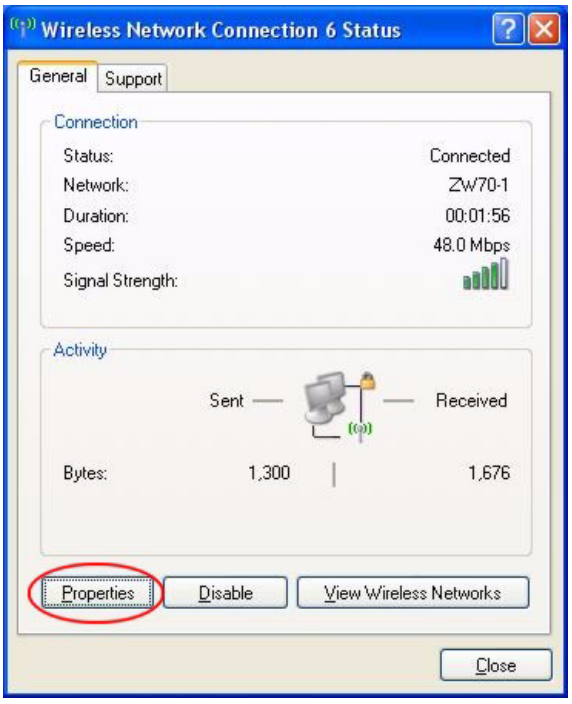



**Figure 104** Windows XP SP2: Wireless Network Connection Status




4 The **Wireless Network Connection Properties** screen displays. Click the **Wireless Networks** tab.

Make sure the **Use Windows to configure my wireless network settings** check box is selected.

**Figure 105** Windows XP SP1: Wireless Network Connection Properties

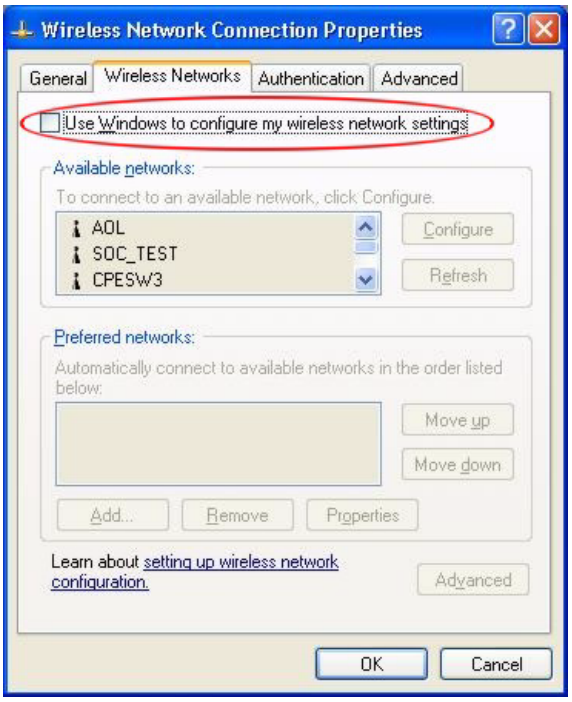
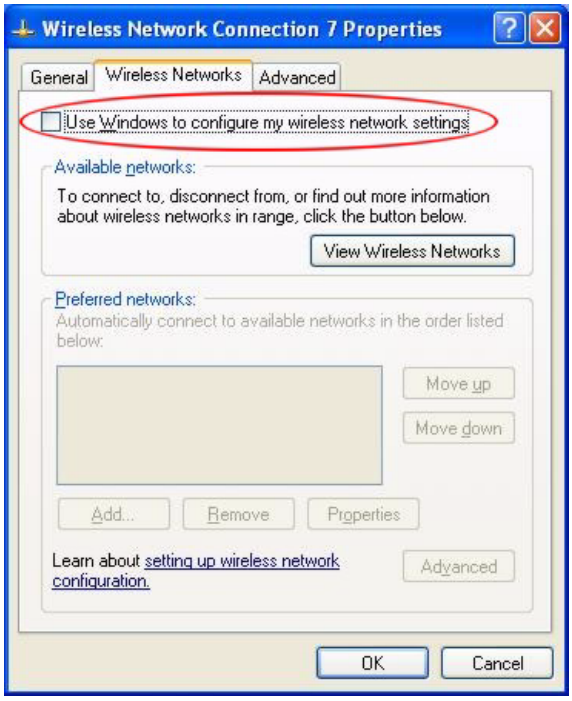
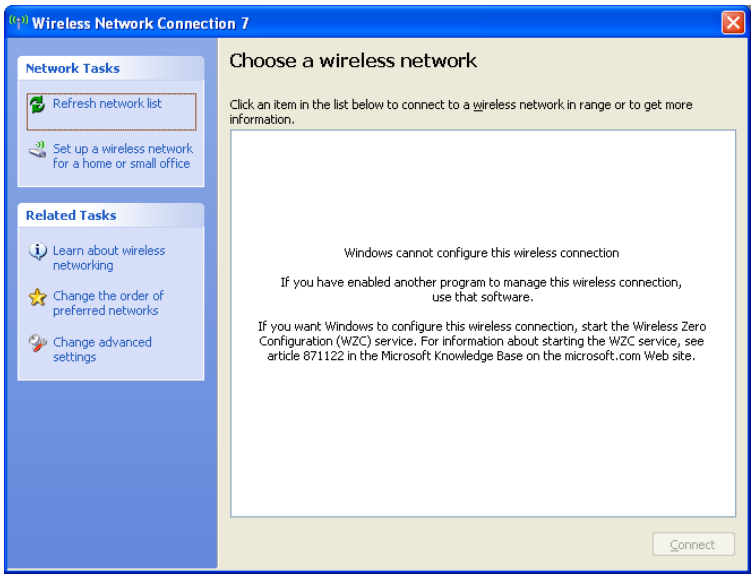



**Figure 106** Windows XP SP2: Wireless Network Connection Properties




If you see the following screen, refer to article 871122 on the Microsoft web site for information on starting WZC.

**Figure 107** Windows XP SP2: WZC Not Available


Wireless Network Connection 7
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Windows cannot configure this wireless connection
If you have enabled another program to manage this wireless connection, use that software.
If you want Windows to configure this wireless connection, start the Wireless Zero Configuration (WZC) service. For information about starting the WZC service, see article 871122 in the Microsoft Knowledge Base on the microsoft.com Web site.
Connect

## Connecting to a Wireless Network

1 Double-click the network icon for wireless connections in the system tray to open the Wireless Network Connection Status screen.

**Figure 108** Windows XP SP2: System Tray Icon

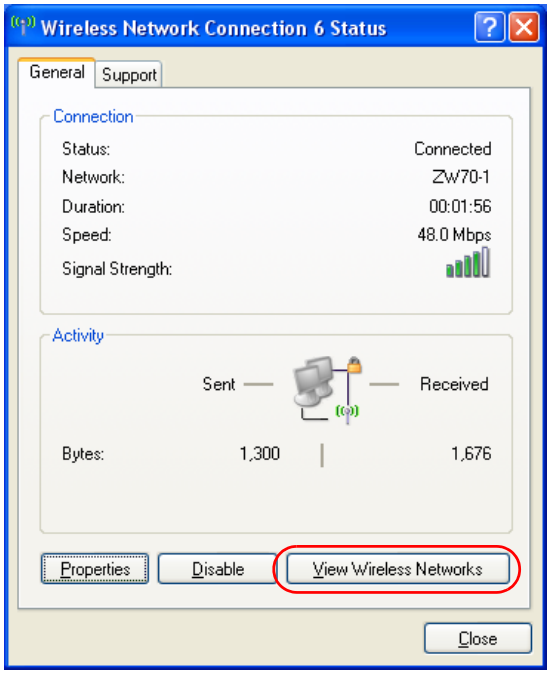
The type of the wireless network icon in Windows XP SP2 indicates the status of the NWD310N. Refer to the following table for details.

**Table 27** Windows XP SP2: System Tray Icon

| ICON | DESCRIPTION |
|---|---|
| | The NWD310N is connected to a wireless network. |
| | The NWD310N is in the process of connecting to a wireless network. |
| | The connection to a wireless network is limited because the network did not assign a network address to the computer. |
| | The NWD310N is not connected to a wireless network. |

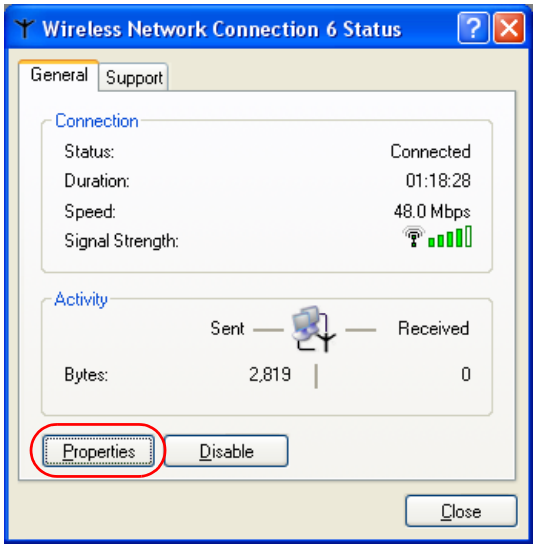
2 Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.

**Figure 109** Windows XP SP2: Wireless Network Connection Status



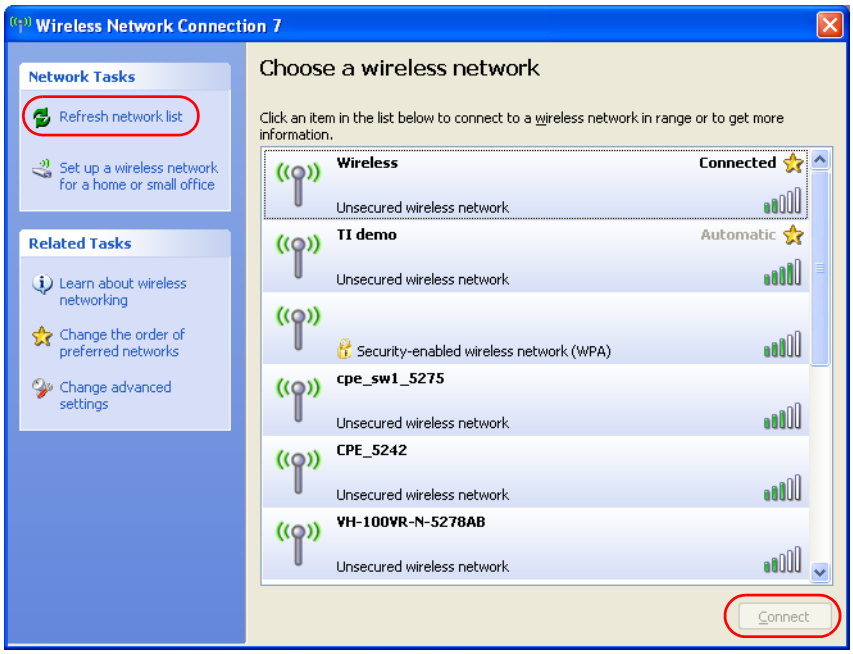

Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.

**Figure 110** Windows XP SP1: Wireless Network Connection Status




3 Windows XP SP2: Click **Refresh network list** to reload and search for available wireless devices within transmission range. Select a wireless network in the list and click **Connect** to join the selected wireless network.

**Figure 111** Windows XP SP2: Wireless Network Connection



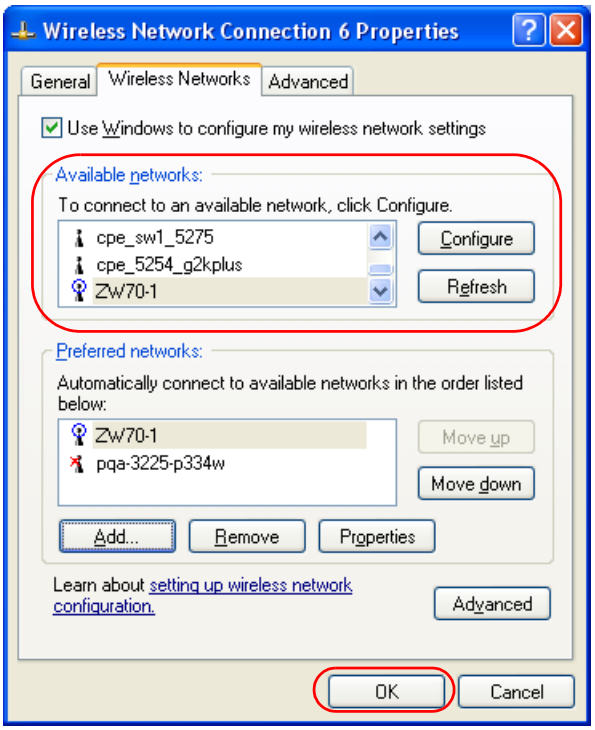

The following table describes the icons in the wireless network list.

**Table 28** Windows XP SP2: Wireless Network Connection

| ICON | DESCRIPTION |
|---|---|
| | This denotes that wireless security is activated for the wireless network. |
| | This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the NWD310N tries to associate to the preferred network first in the order that you specify. Refer to the section on ordering the preferred networks for detailed information. |
| | This denotes the signal strength of the wireless network.<br>Move your cursor to the icon to see details on the signal strength. |

Windows XP SP1: Click **Refresh** to reload and search for available wireless devices within transmission range. Select a wireless network in the **Available networks** list, click **Configure** and set the related fields to the same security settings as the associated AP to add the selected network into the **Preferred** networks table. Click **OK** to join the selected wireless network. Refer to the section on security settings (discussed later) for more information.

**Figure 112** Windows XP SP1: Wireless Network Connection Properties




4 4.Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP and click **Connect**. Refer to the section about security settings for more information. Otherwise click **Cancel** and connect to another wireless network without data encryption. If there is no security activated for the selected wireless network, a warning screen appears. Click **Connect Anyway** if wireless security is not your concern.

**Figure 113** Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK

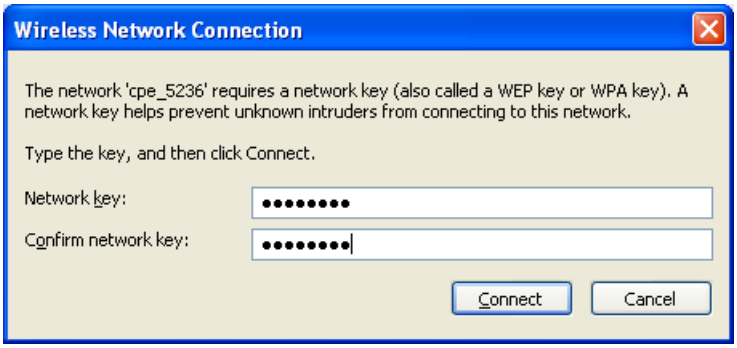

Wireless Network Connection
The network 'cpe_5236' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Confirm network key:
Connect
Cancel

**Figure 114** Windows XP SP2: Wireless Network Connection: No Security

Wireless Network Connection
You are connecting to the unsecured network "CPE_5242". Information sent over this network is not encrypted and might be visible to other people.
Connect Anyway
Cancel

5 Verify that you have successfully connected to the selected network and check the connection status in the wireless network list or the connection icon in the **Preferred networks** or **Available networks** list.

The following table describes the connection icons.

**Table 29** Windows XP: Wireless Networks

| ICON | DESCRIPTION |
|---|---|
| | This denotes the wireless network is an available wireless network. |
| | This denotes the NWD310N is associated to the wireless network. |
| | This denotes the wireless network is not available. |

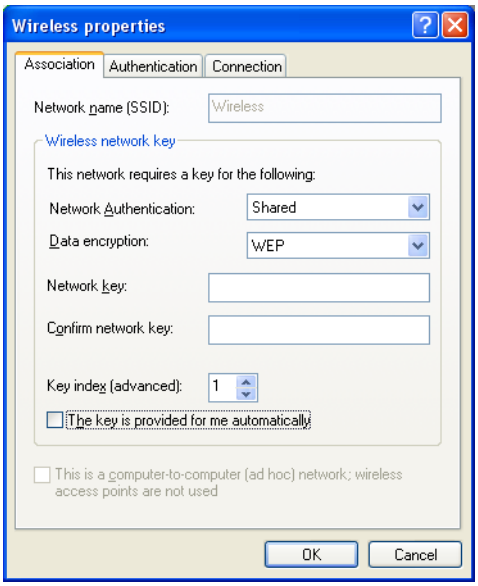
## Security Settings

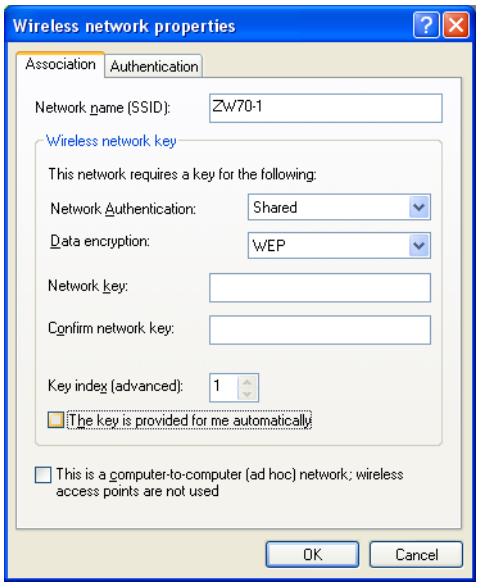
When you configure the NWD310N to connect to a secure network but the security settings are not yet enabled on the NWD310N, you will see different screens according to the authentication and encryption methods used by the selected network.

### Association

Select a network in the Preferred networks list and click Properties to view or configure security.

**Figure 115** Windows XP: Wireless (network) properties: Association



The following table describes the labels in this screen.

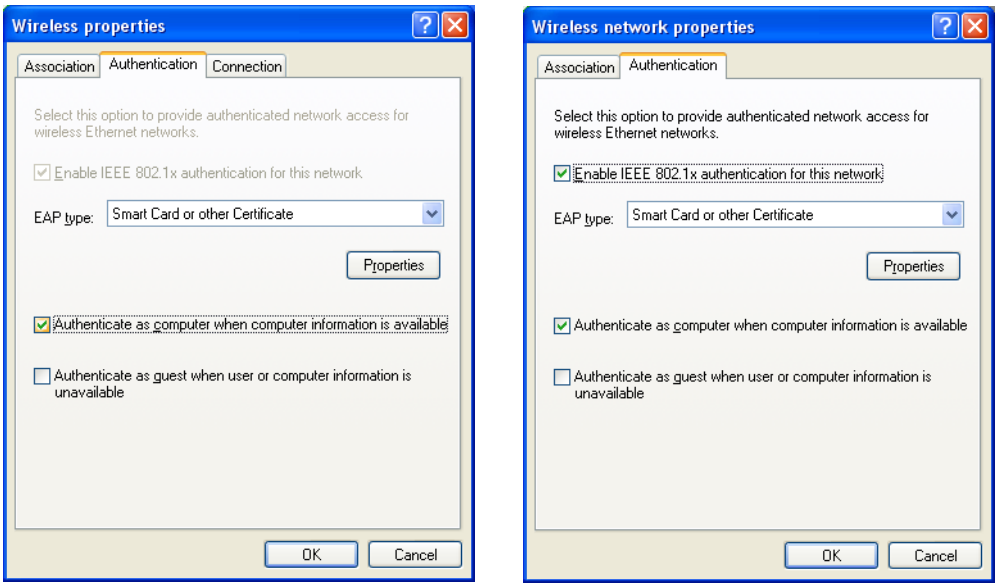
**Table 30** Windows XP: Wireless (network) properties: Association

| LABEL | DESCRIPTION |
|---|---|
| Network name (SSID) | This field displays the SSID (Service Set IDentifier) of each wireless network. |
| Network Authentication | This field automatically shows the authentication method (**Share**, **Open**, **WPA** or **WPA-PSK**) used by the selected network. |
| Data Encryption | This field automatically shows the encryption type (**TKIP**, **WEP** or **Disable**) used by the selected network. |
| Network Key | Enter the pre-shared key or WEP key.<br>The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN. |
| Confirm network key | Enter the key again for confirmation. |
| Key index (advanced) | Select a default WEP key to use for data encryption.<br>This field is available only when the network use **WEP** encryption method and the **The key is provided for me automatically** check box is not selected. |
| The key is provided for me automatically | If this check box is selected, the wireless AP assigns the NWD310N a key. |
| This is a computer-to-computer (ad hoc) network; wireless access points are not used | If this check box is selected, you are connecting to another computer directly. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

### Authentication

Click the **Authentication** tab in the **Wireless (network) properties** screen to display the screen shown next. The fields on this screen are grayed out when the network is in Ad-Hoc mode or data encryption is disabled.

**Figure 116** Windows XP: Wireless (network) properties: Authentication


Wireless properties
Association
Authentication
Connection
Select this option to provide authenticated network access for wireless Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel
Wireless network properties
Association
Authentication
Select this option to provide authenticated network access for wireless Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

The following table describes the labels in this screen.

**Table 31** Windows XP: Wireless (network) properties: Authentication

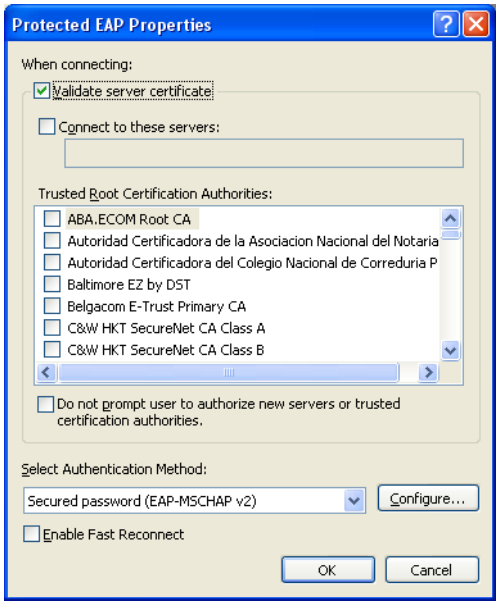
| LABEL | DESCRIPTION |
|---|---|
| Enable IEEE 802.1x authentication for this network | This field displays whether the IEEE 802.1x authentication is active.<br>If the network authentication is set to **Open** in the previous screen, you can choose to disable or enable this feature. |
| EAP Type | Select the type of EAP authentication. Options are **Protected EAP (PEAP)** and **Smart Card or other Certificate**. |
| Properties | Click this button to open the properties screen and configure certificates. The screen varies depending on what you select in the **EAP type** field. |
| Authenticate as computer when computer information is available | Select this check box to have the computer send its information to the network for authentication when a user is not logged on. |
| Authenticate as guest when user or computer information is unavailable | Select this check box to have the computer access to the network as a guest when a user is not logged on or computer information is not available. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

### Authentication Properties

Select an EAP authentication type in the **Wireless (network) properties: Authentication** screen and click the **Properties** button to display the following screen.

### *Protected EAP Properties*

**Figure 117** Windows XP: Protected EAP Properties


Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
ABA.ECOM Root CA
Autoridad Certificadora de la Asociacion Nacional del Notaria
Autoridad Certificadora del Colegio Nacional de Correduria P
Baltimore EZ by DST
Belgacom E-Trust Primary CA
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
OK
Cancel

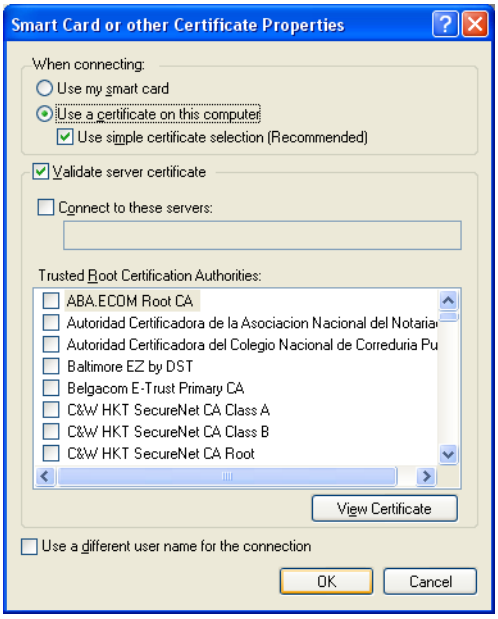
The following table describes the labels in this screen.

**Table 32** Windows XP: Protected EAP Properties

| LABEL | DESCRIPTION |
|---|---|
| Validate server certificate | Select the check box to verify the certificate of the authentication server. |
| Connect to these servers | Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain. |
| Trusted Root Certification Authorities: | Select a trusted certification authority from the list below.<br>Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information. |
| Do not prompt user to authorize new server or trusted certification authorities. | Select this check box to verify a new authentication server or trusted CA without prompting.<br>This field is available only if you installed the Windows XP server pack 2. |
| Select Authentication Method: | Select an authentication method from the drop-down list box and click **Configure** to do settings. |
| Enable Fast Reconnect | Select the check box to automatically reconnect to the network (without re-authentication) if the wireless connection goes down. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

### *Smart Card or other Certificate Properties*

**Figure 118** Windows XP: Smart Card or other Certificate Properties


Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Use simple certificate selection (Recommended)
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
ABA.ECOM Root CA
Autoridad Certificadora de la Asociacion Nacional del Notariat
Autoridad Certificadora del Colegio Nacional de Correduria Pu
Baltimore EZ by DST
Belgacom E-Trust Primary CA
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
C&W HKT SecureNet CA Root
View Certificate
Use a different user name for the connection
OK
Cancel

The following table describes the labels in this screen.

**Table 33** Windows XP: Smart Card or other Certificate Properties

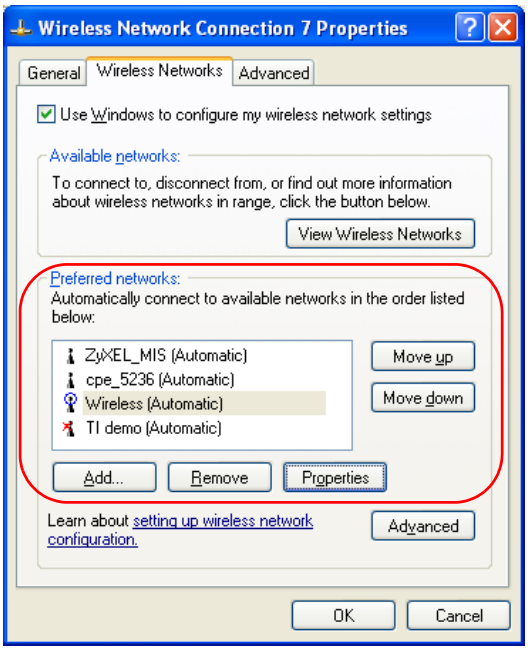
| LABEL | DESCRIPTION |
|---|---|
| Use my smart card | Select this check box to use the smart card for authentication. |
| Use a certificate on this computer | Select this check box to use a certificate on your computer for authentication. |
| Validate server certificate | Select the check box to check the certificate of the authentication server. |
| Connect to these servers | Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain. |
| Trusted Root Certification Authorities: | Select a trusted certification authority from the list below.<br>Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information. |
| View Certificate | Click this button if you want to verify the selected certificate. |
| Use a different user name for the connection: | Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

## Ordering the Preferred Networks

Follow the steps below to manage your preferred networks.

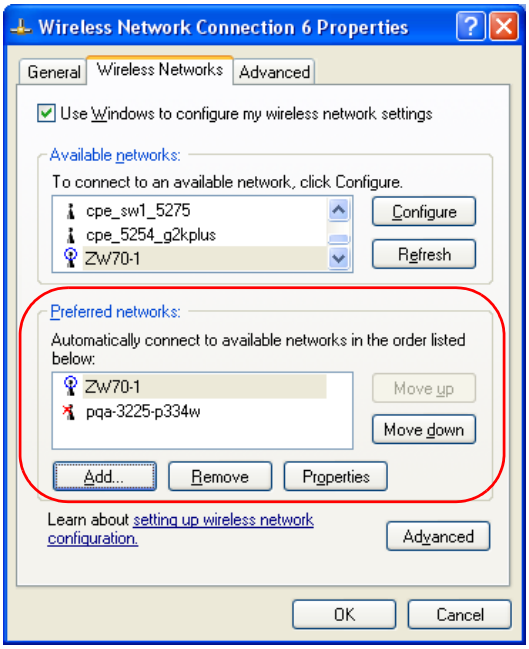
1 Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see Figure 111 on page 129). The screen displays as shown.

**Figure 119** Windows XP SP2: Wireless Networks: Preferred Networks




Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the screen as shown.

**Figure 120** Windows XP SP1: Wireless Networks: Preferred Networks




2 Whenever the NWD310N tries to connect to a new network, the new network is added in the **Preferred networks** table automatically. Select a network and click **Move up** or

**Move down** to change it's order, click **Remove** to delete it or click **Properties** to view the security, authentication or connection information of the selected network. Click **Add** to add a preferred network into the list manually.

# D

# Legal Information

## Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

### Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

## 注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

1. Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.
3 Select the certification you wish to view from this page.

# ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

# E

# Customer Support

Please have the following information ready when you contact customer support.

### Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

### Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

### Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

### Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

### Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

### Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

### Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

### India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

### Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

### Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

### Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

### North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

### Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

### Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

### Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

### Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

### Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

### Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

### Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

### United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

# Index

## A

About 67
about your ZyXEL Device 21
Access Point (AP) 37
Access point (AP) 37
Access Point. See also AP.
ACT LED 22
activating a profile 61
adapter 61
Ad-Hoc 23, 59
Advanced Encryption Standard 39
  See AES.
advanced settings 61
AES 112
antenna
  directional 115
  gain 115
  omni-directional 115
AP 105
  See also access point.
AP MAC address 48
authentication 48
authentication type 39
  auto 39
  open system 39
  shared key 39
auto authentication 39
automatic connection 49
automatic network scan 32, 56

## B

band 77
Basic Service Set, See BSS 103
BSS 103

## C

CA 39, 110
CCMP 39
Certificate Authority
  See CA.
certifications 139
  notices 140
  viewing 140
channel 38, 48, 50, 59, 77, 105
  interference 105
configuration method 25
  important note 25
  Wireless Zero Configuration (WZC) 24, 25
  ZyXEL utility 25
configuration status 47
connection status 47
contact information 143
continuous access mode 62
copyright 139
creating a new profile 58
credentials 65
CTS (Clear to Send) 106
current configuration 47
current connection status 47
customer support 143

## D

data encryption 50
data rate 77
digital ID 39
dimensions 77
disclaimer 139
download 68
driver version 67
dynamic WEP key exchange 111

## E

EAP (Extensible Authentication Protocol) 39
EAP Authentication 109
EAP authentication 39
EAP type 64
EAP-PEAP 39
EAP-TLS 39

EAP-TTLS 39
encryption 112
encryption type 39, 51, 53
environmental specifications 77
ESS 104
Extended Service Set, See ESS 104

## F

fast power save 62
FCC interference statement 139
fragmentation threshold 106
frequency 38, 77

## G

getting started 21

## H

hardware connections 24
help 26
hidden node 105
humidity 77

## I

IBSS 103
IEEE 802.11g 107
IEEE 802.1x 39, 54, 64
Independent Basic Service Set
See IBSS 103
Industrial Scientific Medical Band 77
infrastructure 23
Initialization Vector (IV) 112
installation 24
interface 77
Internet access 23

## L

LEDs 22
lights 22
link information 47
LINK LED 22
link quality 48, 49

## M

manual network connection 32
Message Integrity Check (MIC) 39, 112
modulation 77

## N

network mode 48
network name 48
network overlap 37
network scan 56
network type 48, 50

## O

online help 26
output power 77

## P

packet collisions 49
Pairwise Master Key (PMK) 112, 114
passphrase 38, 51
password 38
PEAP 64
peer computer 23, 59
physical specifications 77
power consumption 77
power saving 62
power saving mode 62
preamble 61
preamble mode 107
product registration 141

product specifications 77
profile 48, 57
activation 61
add new 58
configure 32, 34
default 56
delete 57
edit 57
information 57
new 57, 58
PSK 112

## Q

Quick Start Guide 24, 74

## R

radio band 77
radio interference 74
radio specifications 77
RADIUS 39, 40, 108
message types 109
messages 109
shared secret key 109
real-time data traffic statistics 49
receive rate 48
registration
product 141
related documentation 3
RTS (Request To Send) 106
threshold 105, 106

## S

safety warnings 6
save power 62
scan 49
scan info 59
search 49
security 38, 48, 78
data encryption 38
security settings and Vista 64
sensitivity 78
Service Set Identity (SSID) 32, 37
signal strength 49, 50
site information 50
site survey 49
scan 50
security settings 51
sleep mode 62
SSID 32, 37, 48, 50, 74
statistics 48
syntax conventions 4
system tray 24

## T

temperature 77
Temporal Key Integrity Protocol (TKIP) 39, 112
The 64
TLS 64, 65
total receive 48
total transmit 48
trademarks 139
transmission rate 48, 57
transmit key 51
transmit rate 48
trend chart 48, 49
TTLS 64

## U

uninstalling the ZyXEL utility 67
upgrading the ZyXEL utility 68
important step 69
user authentication 38
utility installation 24
utility version 67

## V

Vista 64, 65
voltage 77

## W

warranty 141
note 141

weight 77
WEP 38, 51
  automatic setup 38
  manual setup 38, 51
  passphrase 38, 51
WEP (Wired Equivalent Privacy) 38
WEP Encryption 51
WEP key generation 38
Wi-Fi Protected Access 39, 111
Wi-Fi Protected Setup 47
Windows 64
Windows XP 25
wireless client 37
wireless client WPA supplicants 113
wireless LAN
  introduction 37
  security 38
wireless LAN (WLAN) 37
wireless network 37
wireless security 107
wireless standard 48, 77
wireless station mode
  adapter 61
  security settings 51
  site survey 49
  trend chart 49
wireless tutorial 27
WLAN
  interference 105
  security parameters 114
WPA 39, 52, 64, 111
  key caching 112
  pre-authentication 112
  user authentication 112
  vs WPA-PSK 112
  wireless client supplicant 113
  with RADIUS application example 113
WPA2 39, 52, 64, 111
  user authentication 112
  vs WPA2-PSK 112
  wireless client supplicant 113
  with RADIUS application example 113
WPA2-Pre-Shared Key 40, 111
WPA2-PSK 40, 52, 111, 112
  application example 113
WPA-PSK 40, 52, 111, 112
  application example 113
WPS
  see also Wi-Fi Protected Setup 47
WZC
  activating 124
  network connection 127
  not available 126
  preferred network 135
  security setting 131
  system tray icon 127
WZC (Wireless Zero Configuration) 25

## Z

ZyXEL Utility
  accessing 26
ZyXEL utility 25
  accessing 26
  driver version number 67
  exiting 25
  help 26
  reactivating 25
  status 25
  system tray icon 24
  upgrading 68
  version number 67